



# Using the Bit9 Security Platform

Bit9 Platform Version: [7.2.1](#)

Document Date: [April 4, 2016](#)



# Copyrights and Notices

Copyright © 2004-2016 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Carbon Black is a trademark of Carbon Black, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW EXCEPT WHEN OTHERWISE STATED IN WRITING. THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Carbon Black, Inc. acknowledges the use of the following third-party software in Bit9 Platform products:

Portions of this software created by gSOAP are Copyright © 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved. SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes PHP, freely available from <http://www.php.net>. Copyright © 1999 - 2010 The PHP Group. All rights reserved. THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software use Info-ZIP, copyright (c) 1990-2007 Info-ZIP. All rights reserved. For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals: Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White. This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions: 1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions. 2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled. 3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions. 4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Portions of this software use RadControls for WinForms, Copyright © 2010-2014, Telerik Corporation. All Rights Reserved. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

This program uses the unRAR utility program. Under no conditions may the code be used to develop a RAR (WinRAR) compatible archiver.

This product contains Smarty and 7-Zip, which are copyrighted software licensed under the Lesser General Public License v3. Copies of the GPL and LGPL licenses can be found at <http://www.gnu.org/licenses/gpl-3.0.html> and <http://www.gnu.org/copyleft/lesser.html>. You may obtain the Minimal Corresponding Source code from us for a period of three years after our last shipment of this product, which will be no earlier than 2015-07-30 by writing to GPL Compliance Division, Carbon Black, Inc., 1100 Winter Street, Waltham, MA 02451.

## *Using the Bit9 Security Platform*

Portions of this software use Chromium, Copyright 2014 The Chromium Authors. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Copyright (c) 2009, CodePlex Foundation All rights reserved.

- Neither the name of CodePlex Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### *Using the Bit9 Security Platform*

Document Version: 7.2.1.i

Document Revision Date: March 21, 2016

Product Version: 7.2.1

### **Carbon Black, Inc.**

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400

Fax: 617.393.7499

Company Website: <http://www.carbonblack.com>

Support E-mail: [support@carbonblack.com](mailto:support@carbonblack.com)

You may also login to the [Support Portal](#) with your user account to obtain assistance.



# Before You Begin

This preface provides a brief orientation to *Using the Bit9 Security Platform*.

**Important Note:** *Bit9, Inc., has changed its name to Carbon Black, Inc. The Bit9 Security Platform has been renamed to Carbon Black Enterprise Protection. However, this document describes a release that retains Bit9 identity in its user interface, and so the document retains this identity as well. Ongoing support and feature development have not changed – just the name. For more information, see our website at [www.carbonblack.com](http://www.carbonblack.com).*

## Sections

Topic	Page
<a href="#">Intended Audience</a>	6
<a href="#">Bit9 Terminology</a>	6
<a href="#">What this Documentation Covers</a>	8
<a href="#">Community Resources</a>	11
<a href="#">Contacting Support</a>	12

## Intended Audience

This documentation provides information for administrators who will operate the Bit9 Console. Staff who manage Bit9 Security Platform activities should be familiar with the Microsoft Windows operating system, web applications, desktop infrastructure (especially in-house procedures for software rollouts, patch management, and antivirus software maintenance), and the effects of unwanted software. In addition, if you intend to use features that integrate Bit9 Security Platform and Active Directory, you should be familiar with Active Directory concepts and use. Although not necessary for day-to-day users of the Bit9 Console, knowledge of SQL Server management is important for whoever is maintaining the Bit9 Security Platform database server at your site.

Bit9 Security Platform administrators should also be familiar with management of the operating systems of clients managed by Bit9 Security Platform, as well as the software installed on them.

## Bit9 Terminology

The following table defines some of the key terms you will need to understand Bit9 Security Platform and its features:

Term	Definition
<b>Bit9 Server</b>	Computer running the Bit9 Server software on a supported Windows platform.
<b>Bit9 Agent</b>	Agent software installed on computers on your network; the agent runs independently but reports to the Bit9 Server.
<b>Bit9 Console</b>	The console, which can be displayed remotely with a web browser, is the user interface and management center for all Bit9 management activities.
<b>Enforcement Level</b>	The protection level applied to computers running the Bit9 Agent. A range of levels from High (Block Unapproved) to None (Disabled) enable you to specify the level of file blocking required.
<b>Computer</b>	Computer that runs the Bit9 Agent. Each Bit9-managed computer is protected by the agent, which both provides information and receives protection updates when it is connected to the Bit9 Server. Virtual machines can be included as computers in the Bit9 Security Platform.
<b>Template</b>	Computer that has the Bit9 Agent pre-installed and will be used to clone one or more computers.
<b>Policy</b>	Each computer protected by the Bit9 Security Platform is associated with a policy that defines its security characteristics. Computers with the same security requirements can share the same policy.
<b>Computer Initialization</b>	File initialization process for new computers that come online to the Bit9 system. During initialization, each file on the fixed drives of the new machine is evaluated and classified by the Bit9 Server.

Term	Definition
<b>Login Account</b>	<p>To use the Bit9 Console, users must have a login account. Role-based accounts tailored to users' responsibilities determine what they can do on the system.</p> <p>Note that users of computers running the Bit9 <i>Agent</i> do not need Bit9 Console accounts. The server requires no direct interaction with users of computers Bit9 is monitoring.</p>
<b>Executables and Scripts</b>	<p>An executable is any file that contains executable code. The Bit9 Security Platform examines the <i>content</i> of each unknown file that appears on a computer in its network, determines whether it contains executable code, and, if so, categorizes it according to executable type.</p> <p>The Bit9 Security Platform has special rules that identify and manage scripts, and you can define additional rules for script identification.</p> <p>The Bit9 Server keeps an inventory of executables and scripts, and provides rules that control whether they are allowed to run. Files not identified as executables or scripts are not inventoried, although you might be able to control access to them with custom rules, such as <i>file integrity rules</i>.</p>
<b>File State</b>	<p>The Bit9 Security Platform classification that determines how executables are tracked and permitted or not permitted to be run. Top-level file states includes approved, banned, and unapproved (neither approved nor banned) states. Files have global and local files states, and these may vary in some cases.</p>
<b>Software Approval</b>	<p>Bit9 Security Platform features for approving legitimate software. Approved software is allowed to run without user or administrator intervention, even on computers "locked down" under high protection.</p>
<b>Reputation</b>	<p>Information that provides guidance about whether a file should be approved or banned. Bit9 Software Reputation Service, which is integrated with the Bit9 Server, provides reputation data for a large database of files and file publishers.</p>
<b>Notifier</b>	<p>A dialog box or transient panel that can appear when a Bit9 rule blocks an action. Notifiers may contain information about why the action was blocked, and in some cases give the user the option of allowing the action or requesting approval from an administrator. Notifiers are be configured and saved by name, and can be attached to different Bit9 rules.</p>
<b>Approval Request</b>	<p>A request by a user whose action was blocked for access to a file or device. Approval requests can be handled informally through email or websites outside of the Bit9 Security Platform, or using the approval request management feature in notifiers and the Bit9 Console.</p>
<b>Drift Report</b>	<p>A report that can help determine how far one or more computers have "drifted" from a baseline of files (by having files added, removed or changed). This can help determine level of compliance with company policies on acceptable files, and also identify files that should be approved and added to an updated baseline.</p>
<b>Live Inventory</b>	<p>Bit9's near-real-time database of all files of interest on all computers running the Bit9 Agent.</p>

Term	Definition
<b>Baseline and Snapshot</b>	A reference point that can be used to determine drift of computers running Bit9 Agent from the reference, and thus potential risk for those computers. A baseline can be a named table of files, called a Snapshot, or the current set of files on a reference computer.
<b>Indicator Set</b>	Groups of rules called “indicators” that aid in detecting particularly threatening or suspicious activity on systems reporting to your Bit9 server.
<b>Health Indicator</b>	A rule that checks whether certain parameters on the Bit9 Server and SQL Server meet the Bit9 operating requirements and reports its results to the System Health page.
<b>Event</b>	Records of actions related to Bit9 activities, including files blocked, unapproved files executed, system management processes and actions by console users. Events may be examined in the Bit9 Console and exported to other analytical tools such as Syslog servers or data analysis systems.
<b>Event Rule</b>	A rule that takes a particular action when a specified event is recorded on the Bit9 Server. Actions include changing file states, uploading files from endpoints, and sending files to third-party detonation engines.

## What this Documentation Covers

*Using the Bit9 Security Platform* is your guide to day-to-day administration tasks: monitoring executable files on your network using the Bit9 Security Platform; configuring the Bit9 Server; managing computers running the Bit9 Agent; and managing Bit9 Console users. It covers the following:

Chapter	Description
<b>1</b> <a href="#">Bit9 Security Platform Overview</a>	Describes the Bit9 Security Platform architecture, key management concepts, and operation strategies.
<b>2</b> <a href="#">Using the Bit9 Console</a>	Describes how to log in to the system and navigate to security platform features using the Bit9 Console. It includes descriptions of common menus and buttons.
<b>3</b> <a href="#">Managing Console Login Accounts</a>	Describes how to create, manage, and delete login accounts. Also describes the privileges of different types of user accounts, and how to use Active Directory accounts as Bit9 Console accounts.
<b>4</b> <a href="#">Creating and Configuring Policies</a>	Describes policies, which define the protections for groups of computers; includes policy settings, Enforcement Levels, and how to change them.
<b>5</b> <a href="#">Managing Computers</a>	Describes how to configure, deploy, and install the Bit9 Agent. Also describes how to get information about Bit9-Security-Platform-managed computers.
<b>6</b> <a href="#">Managing Virtual Machines</a>	Describes special considerations for managing virtual machines created from template computers.

Chapter	Description
7 <a href="#">File and Publisher Information</a>	Describes where and how you get information about files seen by the Bit9 Security Platform. Includes descriptions of the detailed global and local file state information provided by the Bit9 Security Platform.
8 <a href="#">Approving and Banning Software</a>	Describes different methods of approving and banning files, and when to use them.
9 <a href="#">Reputation Approval Rules</a>	Describes how to use Bit9 Software Reputation Service trust settings to automatically approve files and publishers.
10 <a href="#">Managing File-Signing Certificates</a>	Describes how approve and ban files by approving or banning specific certificates associated with a publisher.
11 <a href="#">Managing Devices</a>	Describes how to set up rules to control access to files on devices connected to computers.
12 <a href="#">Custom Software Rules</a>	Describes how to create “custom rules” that affect what happens when there is an attempt to execute or write files at specified paths. Also describes how to export rules from one server and import them to another.
13 <a href="#">Script Rules</a>	Describes how to add files to the list of those controlled by Bit9 Security Platform script rules.
14 <a href="#">Registry Rules</a>	Describes how to create registry rules that affect what happens when there is an attempt to modify the Windows Registry at specified paths.
15 <a href="#">Memory Rules</a>	Describes how to create rules that affect what happens when there is an attempt by one process to access or alter another process.
16 <a href="#">Event Rules</a>	Describes how to create rules that take a specified action when specified events are reported to the Bit9 Server.
17 <a href="#">Block Notifiers and Approval Requests</a>	Describes how blocked file notifiers work on agent computers and describes how to customize notifiers. Also describes configuration and management of approval requests from users.
18 <a href="#">Events, Alerts and Meters</a>	Describes how to carry out day-to-day monitoring operations. Instructions include how to use Bit9 Security Platform reports and events to identify changes in network file activity and respond appropriately. Also describes how to set up email alerts for Bit9-monitored activity, and how to meter execution of specific files.
19 <a href="#">Monitoring Change: Baseline Drift Reports</a>	Describes how to use the Baseline Drift Report feature to monitor change in file inventory over time.
20 <a href="#">Advanced Threat Detection</a>	Describes Bit9’s advanced threat indicators, which can be used to detect threatening or suspicious activity on systems reporting to your Bit9 Server

Chapter	Description
<b>21</b> <a href="#">Using and Customizing Dashboards</a>	Describes Bit9 Dashboards, special graphic displays that summarize key information about Bit9-Security-Platform-managed computers and the files on them.
<b>22</b> <a href="#">Locating Files</a>	Describes the Find Files feature, which can locate specific executable files on computers running the Bit9 Agent on your network.
<b>23</b> <a href="#">System Configuration</a>	Describes configuration settings, including integration with other servers (including Carbon Black), backup procedures, product update procedures, optional Bit9 Software Reputation Service hash-identification services, agent-server communication security, and other configuration options.
<b>23</b> <a href="#">Monitoring System Health</a>	Describes the System Health page, which provides information about factors that affect the health of your Bit9 Platform environment, including compliance with the hardware and software requirements, SQL Server configuration, and other health and performance data.
<b>A</b> <a href="#">Live Inventory SDK: Database Views</a>	Describes the set of available read-only views into the "live inventory" database of files on your Bit9-managed computers.
<b>B</b> <a href="#">Bit9 API</a>	Describes the Bit9 API, a RESTful API that may be used to write code to interact with Bit9 Platform, either using custom scripts or from other applications, including network security platforms.
<b>C</b> <a href="#">Bit9 Connector for Network Security Devices</a>	Describes the optional, separately licensed connector for integrating third-party network security devices (Check Point, Palo Alto Networks, FireEye) with the Bit9 Security Platform.
<b>D</b> <a href="#">Diagnostic Files</a>	Describes how to upload and access agent diagnostic files. Also describes server diagnostic files available through the console.
<b>E</b> <a href="#">Uploading Files from Agents</a>	Describes the optional, separately licensed features for uploading files from agents to the server.
<b>F</b> <a href="#">Exporting Bit9 Data for External Analysis</a>	Describes the optional, separately licensed features for sending endpoint data collected by the Bit9 Server collects to external analysis tools such as Splunk.

## Other Bit9 Documentation

You will need some or all of the following Bit9 documentation to accomplish tasks not covered in *Using the Bit9 Security Platform*. These documents may have been downloaded with the Bit9 Server installer; they are available on the Bit9 customer portal.

Some of these documents are updated with every new released build while others are updated only for minor or major version changes:

- ***Operating Environment Requirements*** – This describes the hardware and software platform requirements for Bit9 Server, the SQL Server database that stores Bit9 data, and the Bit9 Agent.
- ***Supported Agent Operating Systems*** – This describes the supported operating systems for the current version of the Bit9 Agent.
- ***Installing Bit9 Server*** – This includes instructions for initial installation of the Bit9 Server and for upgrades of the server from previous releases. Note that installation of Bit9 Agents is described in this document (*Using the Bit9 Security Platform*).
- ***Bit9 Security Platform Release Notes*** – This document is specific to the version and build of Bit9 Server you received. It contains information about new features, corrective content, and known issues with the release.
- ***Bit9 Events Integration Guide*** – This document provides a detailed inventory of events recorded by the Bit9 Server and includes instructions for integrating Bit9 event data with third-party SIEM systems via Syslog.

If you are new to the advanced threat environment, you might find *Next Generation Endpoint Security For Dummies (Carbon Black Edition)*, by Mike Chapple, a useful overview. It is available as a free PDF download at the following URL:

<https://www.carbonblack.com/files/ebook-next-generation-endpoint-security-for-dummies/>

## Community Resources

The Carbon Black User eXchange website at <https://community.carbonblack.com> provides access to information shared by Carbon Black customers, employees and partners. It includes information and community participation for users of all Carbon Black products including Carbon Black Enterprise Protection (formerly Bit9 Platform) and Carbon Black Enterprise Response (formerly Carbon Black).

When you login to this resource, you can:

- ask questions and provide answers to other users' questions
- “vote” to bump up the status of product ideas
- download the latest user documentation
- participate in the Carbon Black developer community by posting ideas and solutions or discussing those posted by others
- view the training resources available for Carbon Black products

You must have a login account to access the User eXchange. Contact your Technical Support representative if you need to get an account.

## Contacting Support

For your convenience, our Technical Support offers several channels for resolving support questions related to the Bit9 Platform:

### Technical Support Contact Options

**Web:** [Support Portal](#)

**Email:** [support@carbonblack.com](mailto:support@carbonblack.com)

**Phone:** 877.248.9098

**Fax:** 617.393.7499

**Hours:** 8 a.m. to 8 p.m. EST

## Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

Required Information	Description
<b>Contact</b>	Your name, company name, telephone number, and email address
<b>Product version</b>	Product name and version number
<b>Hardware configuration</b>	Hardware configuration of the server or computer the product is running on (processor, memory, and RAM)
<b>Document version</b>	For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page, or for longer manuals, after the Copyrights and Notices section of the manual.
<b>Problem</b>	Action causing the problem, error message returned, and any other appropriate output
<b>Problem severity</b>	Critical, serious, minor, or enhancement



# Contents

<b>Copyrights and Notices</b> . . . . .	<b>3</b>
<b>Before You Begin</b> . . . . .	<b>5</b>
Intended Audience . . . . .	6
Bit9 Terminology . . . . .	6
What this Documentation Covers . . . . .	8
Other Bit9 Documentation . . . . .	10
Community Resources . . . . .	11
Contacting Support . . . . .	12
Reporting Problems . . . . .	12
<b>1 Bit9 Security Platform Overview</b> . . . . .	<b>33</b>
What is the Bit9 Security Platform? . . . . .	34
How the Bit9 Security Platform Works . . . . .	38
Files Tracked by the Bit9 Security Platform . . . . .	39
System Architecture . . . . .	39
Bit9 Server . . . . .	40
Integrating Bit9 Security Platform with Active Directory . . . . .	40
Bit9 Agent . . . . .	40
Trust Rating from Bit9 Software Reputation Service . . . . .	40
File State, Whitelisting and Blacklisting . . . . .	41
Global State . . . . .	41
Local State . . . . .	42
File Approval Methods . . . . .	42
File Ban Methods . . . . .	42
Custom Rules . . . . .	43
Security Policies and Levels . . . . .	43
Policy Settings . . . . .	44
Modes and Enforcement Levels . . . . .	44
Bit9 Security Platform Licensing and Modes . . . . .	45
Operating Strategies . . . . .	45
<b>2 Using the Bit9 Console</b> . . . . .	<b>47</b>
Logging In . . . . .	48
Login, Server, Version and Alert Information . . . . .	49
Logging Out . . . . .	49
The Home Page . . . . .	50
Using the Main Menu . . . . .	53
Left Navigation Menu and Breadcrumbs . . . . .	57
Bit9 Console Tables . . . . .	58

Table Data Control Links . . . . .	59
Table Column Resizing . . . . .	59
Row Action Buttons . . . . .	59
Checked Row Action Menus . . . . .	60
Row Rank Arrows . . . . .	61
“Add” Buttons . . . . .	61
Pages, Tabs and Saved Views . . . . .	62
Filter Options . . . . .	62
Show/Hide Columns Options . . . . .	64
Tabs . . . . .	65
Table Length . . . . .	65
Default and Saved Views . . . . .	66
Exporting Bit9 Server Data to Files . . . . .	68
Details Pages and Object Previews . . . . .	68
Menus on Details Pages . . . . .	69
Object Previews in Table Data . . . . .	70
Shortcut Links . . . . .	71
Setting Preferences for Console Users . . . . .	71
Using Context-Sensitive Help . . . . .	73
<b>3 Managing Console Login Accounts . . . . .</b>	<b>75</b>
Login Account Management . . . . .	76
Account Group and Access Privileges . . . . .	76
Enabling Console Access via AD Accounts . . . . .	77
AD Login Account Format . . . . .	79
Adding, Deleting, and Changing AD Login Accounts . . . . .	80
Changing AD Group Mapping and Rank . . . . .	81
Changing AD User Details Displayed in the Bit9 Console . . . . .	82
Creating Login Accounts through Bit9 Console . . . . .	83
Changing Passwords and Other Account Details . . . . .	85
Deleting Login Accounts . . . . .	87
Disabling Login Accounts . . . . .	88
Managing Console Account Groups . . . . .	89
Changing AD Mapping and Rank of a Group . . . . .	89
Creating a New Login Account Group . . . . .	90
Account Group Permissions . . . . .	93
Editing a Login Account Group . . . . .	97
Disabling a Group . . . . .	97
Deleting a Group . . . . .	98
<b>4 Managing Computers . . . . .</b>	<b>99</b>
Computer Configuration Overview . . . . .	100
Pre-Installation Activities . . . . .	100
Installation and Initialization . . . . .	100
Post-Installation Activities . . . . .	101

Access to Computer Management Features . . . . .	102
Assigning Computers to a Policy . . . . .	102
Assigning Policy by Active Directory Mapping . . . . .	103
AD Policy Mapping Summary . . . . .	103
Creating AD Mapping Rules . . . . .	104
Mapping Rule Ranking . . . . .	109
AD Object Browser Options . . . . .	109
Computer Registration and AD Mapping . . . . .	111
Clearing the Server AD Cache . . . . .	111
Viewing AD Computer Details in the Bit9 Console . . . . .	111
Downloading Agent Installers . . . . .	112
Installing Bit9 Agents . . . . .	113
Preparing for New Agent Installation . . . . .	113
Installing the Agent on a Windows Computer . . . . .	114
Installing the Agent on a Mac Computer . . . . .	116
Installing the Agent on a Linux Computer . . . . .	117
Verifying the Installation . . . . .	119
Verifying Installation on the Agent Computer . . . . .	119
Upgrading Bit9 Agents . . . . .	119
Feature Limitations for Non-Upgraded Agents . . . . .	120
Enabling Automatic Agent Upgrades . . . . .	121
Upgrading Immediately from the Bit9 Console . . . . .	121
Manually Upgrading Agents . . . . .	122
Manually Upgrading Windows Agents . . . . .	123
Manually Upgrading Mac Agents . . . . .	124
Manually Upgrading Linux Agents . . . . .	125
Agent Upgrade Status . . . . .	125
Uninstalling Bit9 Agents . . . . .	127
Uninstalling the Agent from a Windows Computer . . . . .	127
Uninstalling the Agent from a Mac Computer . . . . .	128
Uninstalling the Agent from a Linux Computer . . . . .	128
Viewing the Table of Computers . . . . .	128
Agent Policy Status . . . . .	130
Actions on Selected Computers . . . . .	131
Viewing Complete Details for One Computer . . . . .	132
Moving Computers to Another Policy . . . . .	143
Restoring Computers from the Default Policy . . . . .	144
Moving a Computer to Local Approval Mode . . . . .	146
Adding Computers . . . . .	146
Deleting Computers . . . . .	146
Duplicate Computers . . . . .	147
<b>5 Creating and Configuring Policies . . . . .</b>	<b>149</b>
Policy and Enforcement Level Overview . . . . .	150
Creating Policies . . . . .	151

Policy Settings . . . . .	156
Advanced Settings . . . . .	156
Template Policy and Default Policy . . . . .	160
Default Policy . . . . .	160
Template Policy . . . . .	161
Resetting a Policy to Template Policy Settings . . . . .	162
Tamper-Protection Setting . . . . .	162
Editing a Policy . . . . .	163
Related Views in Policy Details . . . . .	165
Enforcement Levels . . . . .	166
How Enforcement Levels Affect Policy Setting Enforcement . . . . .	167
Special Enforcement Level for Local Approval . . . . .	169
Changing Policy Enforcement Levels . . . . .	169
Locking Down all Computers . . . . .	171
Deleting Policies . . . . .	173
<b>6 Managing Virtual Machines . . . . .</b>	<b>175</b>
Overview . . . . .	176
Creating a Template Computer . . . . .	177
Viewing Templates in the Computers Table . . . . .	178
Viewing and Editing Template Details . . . . .	179
Deploying Clones . . . . .	182
Viewing Clones in the Computers Table . . . . .	182
Finding the Clones for a Template . . . . .	183
Finding the Template for a Clone . . . . .	183
Server Backlog for Clones . . . . .	183
Making Changes to a Template . . . . .	184
Deleting a Template . . . . .	185
Configuring Clone Inventory . . . . .	185
Choosing an Inventory Option . . . . .	186
Deleting Clones . . . . .	187
Manual Cleanup of Clones . . . . .	188
Automatic Cleanup for All Clones . . . . .	188
Automatic Clone Cleanup for One Template . . . . .	189
Converting a Template to a Regular Computer . . . . .	189
<b>7 File and Publisher Information . . . . .</b>	<b>191</b>
Overview . . . . .	192
Viewing File Tables . . . . .	193
File Catalog . . . . .	193
Files on Computers . . . . .	195
Showing Individual Files . . . . .	195
Initialized Files . . . . .	196
Menus on the File Tables Pages . . . . .	197
Finding Computers With or Without Specified Files . . . . .	197

Excluding Tracking of Microsoft Support Files . . . . .	198
Files Instances Affected . . . . .	200
Changes that Affect OS Inventory Tracking . . . . .	200
Information about Excluded File Instances . . . . .	201
File Groups . . . . .	202
Viewing Details Pages . . . . .	203
File Details Page . . . . .	204
File Instance Details Page . . . . .	210
Menus on the Files Pages . . . . .	213
Menus on the File Details Page . . . . .	213
Menus on the File Instance Details Page . . . . .	213
Summary of File Views . . . . .	215
Global File State . . . . .	217
Flags . . . . .	217
Local File State . . . . .	218
Local State Details . . . . .	219
Publisher Information . . . . .	220
<b>8 Approving and Banning Software . . . . .</b>	<b>223</b>
What is Bit9 Software Approval? . . . . .	<b>224</b>
Platform Considerations for Rule Specifications . . . . .	226
What are Bit9 Software Bans? . . . . .	226
File Ban Options . . . . .	227
Approving by Trusted Directory . . . . .	228
Windows Trusted Directories . . . . .	229
Archives and Installers in Trusted Directories . . . . .	229
Mac and Linux Trusted Directories . . . . .	229
Creating a Trusted Directory . . . . .	230
Verifying Trusted Directories . . . . .	232
Verifying Approval of Windows Packages . . . . .	233
Custom Rules for Installer Access . . . . .	233
Removing or Disabling Directory Trust . . . . .	233
Approving by Trusted User or Group . . . . .	234
How Groups are Specified . . . . .	234
Creating a Trusted User or Group . . . . .	234
Removing Trust from a User or Group . . . . .	236
Approving or Banning by Publisher . . . . .	236
Publisher Approvals . . . . .	237
Publisher Bans . . . . .	237
Managing Bans and Approvals from the Publishers Tab . . . . .	238
Managing Bans and Approvals from the Publishers Details Page . . . . .	240
Adding Publishers . . . . .	241
Removing Publisher Approvals . . . . .	242
Removing Publisher Bans . . . . .	242
Finding All Files from a Publisher . . . . .	242

Determining Which Certificates Can Approve Files .....	242
Approval with Expired Certificates .....	244
Excluding Certificate Algorithms .....	245
Minimum Key Size .....	245
Countersignature Options .....	245
Revocation Checks .....	245
Approving by Updater .....	246
Allowing or Disabling Automatic Updater Updates .....	251
Adding an Updater .....	251
Updater History .....	252
Locally Approving Files .....	252
Automatic Local Approval on Enforcement Level Change .....	253
Which Files Are Locally Approved On Transition .....	255
Locally Approving Individual Files .....	255
Removing Local Approval .....	256
Locally Approving Files Not Yet in File Catalog Inventory .....	256
Locally Approving Transient or Deleted Files .....	257
Locally Approving All Unapproved Files on a Computer .....	257
Moving Computers to Local Approval Mode .....	258
Moving Online Computers into Local Approval Mode .....	259
Restoring Online Computers from Local Approval Mode .....	261
Using Timed Policy Overrides .....	262
Marking a File as an Installer/Not an Installer .....	265
File-Specific Rules: Approvals and Bans .....	266
Report Only Bans .....	268
Creating an Approval or Ban from the Software Rules Page .....	269
Editing and Deleting File Rules .....	271
Creating File Approvals and Bans from Table Pages .....	272
Creating Global Approvals and Bans .....	273
Custom Approvals and Bans .....	274
Warnings when Creating or Editing Bans .....	275
Approving and Banning Files from the File Details Page .....	276
Approving or Banning Lists of Files .....	277
Enabling Bans to Stop Running Processes .....	279
<b>9 Reputation Approval Rules .....</b>	<b>281</b>
Overview .....	282
Trust Ratings for Files and Publishers .....	282
File Trust Ratings .....	282
Publisher Trust Ratings .....	283
Reputation Approval Strategy .....	283
Setting the Trust Level for Approvals .....	284
How File Reputation Approvals Work .....	284
Removal of Reputation Approval for a File .....	285

How Publisher Reputation Approvals Work . . . . .	285
Removal of Reputation Approval for a Publisher . . . . .	285
Reputation Approvals and Other Bit9 Rules . . . . .	286
Creating Exceptions for Files and Publishers . . . . .	286
Disabling Reputation Approvals for a File. . . . .	286
Disabling Reputation Approvals for a Publisher . . . . .	287
Enabling Reputation Approvals . . . . .	287
Modifying and Disabling Reputation Approvals . . . . .	289
Views Related to Reputation Approvals. . . . .	290
<b>10 Managing File-Signing Certificates . . . . .</b>	<b>293</b>
Overview . . . . .	294
Summary of Certificate Management Features . . . . .	295
Viewing Certificate Information. . . . .	295
Certificates Table . . . . .	295
Searching, Sorting and Grouping on the Certificates Table. . . . .	299
Certificate Details. . . . .	300
Related Views Menu on Certificate Details . . . . .	301
Viewing Certificates for a Publisher . . . . .	301
Certificate Fields in File/File Instance Details . . . . .	302
Certificate Alerts . . . . .	303
Certificate Events . . . . .	303
Certificates in External Views . . . . .	304
Using Certificates for Enforcement . . . . .	304
Certificate Approval Configuration Choices . . . . .	304
Certificate Types . . . . .	305
Path Position and Agent Differences . . . . .	306
Approving or Banning Certificates for a Publisher . . . . .	306
Certificate Global State . . . . .	308
Mixed and By-Policy States. . . . .	313
Certificate Ban Setting in Policies. . . . .	313
Interactions with Other Rules . . . . .	313
How Certificate Global State Affects Global File State. . . . .	314
Agent Version and Global File State . . . . .	314
<b>11 Managing Devices . . . . .</b>	<b>315</b>
Overview . . . . .	316
Devices Managed by Bit9 . . . . .	316
Enabling Per-Policy Device Control. . . . .	317
Managing Specific Devices . . . . .	320
Viewing Device Information . . . . .	320
Managing Devices by Model . . . . .	321
Viewing Device Models in the Device Catalog. . . . .	321
Viewing Details for One Device Model . . . . .	322
Approving and Banning Device Models . . . . .	324

Managing Device Instances . . . . .	325
Viewing Instances in the Device Catalog . . . . .	326
Viewing Details for One Device Instance . . . . .	327
Approving or Banning Device Instances . . . . .	328
Managing Computer-Device Attachments . . . . .	330
Viewing Devices on Computers . . . . .	330
Viewing Details for One Computer-Device Attachment . . . . .	332
<b>12 Custom Software Rules . . . . .</b>	<b>335</b>
Overview . . . . .	336
Rule Types . . . . .	336
Rule Scope . . . . .	336
File and Process Matching . . . . .	337
Pre-configured Rules . . . . .	337
Internal Rules in the Custom Rule Table . . . . .	337
Specifying the Notifier for a Custom Rule . . . . .	337
Custom Rules in Visibility Mode . . . . .	338
Creating a Custom Rule . . . . .	338
Custom Rule Parameters . . . . .	341
Specifying Execute and Write Actions . . . . .	342
Specifying Paths and Processes . . . . .	345
Specifying a File or Directory . . . . .	346
Platform-Specific Syntax . . . . .	346
Using Wildcards . . . . .	346
Automatic Path Conversions . . . . .	347
Specifying Devices in Paths in Windows Rules . . . . .	347
Using Macros . . . . .	347
Path Macros . . . . .	348
Windows Registry Macros . . . . .	351
Entering Multiple Paths or Processes . . . . .	352
Specifying Processes . . . . .	353
Specifying Users or Groups . . . . .	353
Rule Ranking . . . . .	354
Rule Ranking and Internal Rules . . . . .	356
Disabling or Deleting Custom Rules . . . . .	357
Viewing Rule Status on Computers . . . . .	358
Exporting and Importing Rules . . . . .	359
Exporting Rules . . . . .	360
Importing Rules . . . . .	361
Selecting Rules to Import . . . . .	362
Differences in Settings for Imported Rules . . . . .	363
Custom Rule Types and Examples . . . . .	366
File Integrity Control . . . . .	366
Trusted Paths . . . . .	367
Execution Control . . . . .	369



File Creation Control .....	371
Performance Optimization .....	371
Pairing Ignore and Block Rules .....	373
<b>13 Script Rules .....</b>	<b>375</b>
Overview .....	376
What is a Script? .....	376
What Bit9 Script Rules Do .....	376
Pre-configured Script Rules .....	377
Script Rules Priority vs. Other Bit9 Rules .....	379
Shell Scripts Identified by Content .....	379
Policy Settings for Script Rules .....	380
Creating a Custom Script Rule .....	380
Editing a Script Rule .....	383
Disabling or Deleting a Script Rule .....	383
Viewing Rule Status on Computers .....	384
Script Rule Examples .....	385
Example: Windows Perl Scripts .....	385
Example: Windows Batch Scripts .....	386
Example: Linux Shell Scripts .....	387
<b>14 Registry Rules .....</b>	<b>389</b>
Overview .....	390
Rule Scope .....	390
Sample Rules .....	390
Exporting and Importing Registry Rules .....	390
Specifying the Notifier for Registry Rules .....	391
Creating Registry Rules .....	391
Registry Rule Parameters .....	394
Specifying a Write Action .....	396
Specifying Registry Paths .....	397
Using Wildcards .....	397
Specifying Keys or Values .....	398
Specifying Processes in Registry Rules .....	398
Specifying Processes or Directories .....	400
Using Wildcards .....	400
Automatic Process Path Conversions .....	400
Specifying Devices in Process Path .....	400
Using Macros .....	401
Entering Multiple Paths or Processes .....	401
Specifying Users or Groups .....	402
Rule Ranking .....	402
Disabling or Deleting Registry Rules .....	403
Viewing Rule Status on Computers .....	403
Sample Registry Rules .....	404

Example: Report Changes to Internet Explorer Trusted Zone . . . . .	404
Autostart Rules . . . . .	406
<b>15 Memory Rules . . . . .</b>	<b>407</b>
Overview . . . . .	408
Rule Scope . . . . .	408
Exporting and Importing Memory Rules . . . . .	409
Specifying the Notifier for Memory Rules . . . . .	409
Creating Memory Rules . . . . .	409
Memory Rule Parameters . . . . .	411
Specifying the Rule Action . . . . .	413
Specifying the Rule Permissions . . . . .	414
Specifying Target and Source Processes . . . . .	415
Specifying a File or Directory . . . . .	415
Using Wildcards . . . . .	416
Automatic Path Conversions . . . . .	416
Specifying Devices in Paths . . . . .	416
Using Macros . . . . .	417
Entering Multiple Target or Source Processes . . . . .	417
The Source Process Menu . . . . .	418
Specifying Users or Groups . . . . .	418
Rule Ranking . . . . .	419
Disabling or Deleting Memory Rules . . . . .	420
Viewing Rule Status on Computers . . . . .	420
<b>16 Event Rules . . . . .</b>	<b>423</b>
Overview . . . . .	424
Events That Can Trigger Rule Actions . . . . .	424
Actions A Rule Can Take . . . . .	424
Simulating the Effect of a Rule . . . . .	425
Re-Applying a Rule to Past Events . . . . .	425
Enabling, Disabling, and Deleting Event Rules . . . . .	425
Disabling Processing of All Event Rules . . . . .	426
Testing a Rule before Enabling . . . . .	427
Creating and Editing Event Rules . . . . .	428
Editing an Event Rule . . . . .	434
Edit Event Rule Page Menus . . . . .	434
Event Rule Ranking . . . . .	435
File and Process Properties in Event Rule Definitions . . . . .	435
Bit9 SRS Trust and Threat Data . . . . .	435
File Prevalence . . . . .	435
File Metadata . . . . .	435
File Extension . . . . .	436
Analysis Results Options . . . . .	436
Global Bans for Non-Cataloged Files . . . . .	436

How Event Rule Approvals Affect Endpoints . . . . .	437
Event Rule History and Processed Events List . . . . .	437
Sample Event Rules . . . . .	438
Sample Rule: Analyze files from approval requests . . . . .	439
Sample Rule: Resolve approval requests for clean files . . . . .	439
Sample Rule: Analyze downloaded files . . . . .	440
Sample Rule: Report malicious files . . . . .	440
<b>17 Block Notifiers and Approval Requests . . . . .</b>	<b>441</b>
Notifiers: What Users See . . . . .	442
Prompt Notifiers . . . . .	442
Block-only Notifiers . . . . .	443
Block Notifiers on Windows Computers . . . . .	444
Block Notifiers on Mac and Linux Computers . . . . .	444
Notifier Components . . . . .	445
Bit9 Notifier Tray Icon and History Window . . . . .	446
Bit9 Notifier History Window . . . . .	446
The Bit9 Console Notifiers Page . . . . .	447
Assigning Notifiers to Settings and Rules . . . . .	447
Assigning Notifiers to Policy Settings . . . . .	447
Policy Settings with Notifiers . . . . .	449
Assigning Notifiers to Custom, Registry and Memory Rules . . . . .	449
Customizing and Creating Notifiers . . . . .	450
Creating a New Notifier . . . . .	453
Editing Notifier Text . . . . .	453
Using Tags in Notifier Text . . . . .	454
Conditional Messages for Block vs. Prompt . . . . .	455
Informational Tags as Conditional Operators . . . . .	457
Editing the Notifier Link . . . . .	458
Tags in Notifier Links . . . . .	458
Editing the Notifier Source Line . . . . .	460
Specifying a Custom Notifier Logo . . . . .	460
Image File Requirements . . . . .	462
Logo-Related Events . . . . .	462
Changing the Logo Image . . . . .	462
Suppressing the Notifier Logo in a Policy . . . . .	462
Resetting a Notifier to Initial Settings . . . . .	462
Resetting a Policy to Initial Notifiers . . . . .	463
Disabling Bit9 Notifiers . . . . .	463
Notifiers in Windows Session Virtualization . . . . .	464
Approval Requests and Justifications . . . . .	467
Enabling Requests and Justifications . . . . .	468
Submitting Requests and Justifications . . . . .	469
Viewing Requests and Justifications . . . . .	470
Resolving Requests and Justifications . . . . .	471

Notifying Users of Approval Request Resolution . . . . .	473
Approval Request and Justification Details . . . . .	476
Customizing the Request/Justification Interface in Notifiers. . . . .	479
<b>18 Events, Alerts and Meters . . . . .</b>	<b>481</b>
Monitoring Prerequisites. . . . .	482
Event Reports . . . . .	482
Using the Home Page Event Reports Portlet . . . . .	483
Viewing Reports on the Events Page . . . . .	484
Object Previews in Events Tables . . . . .	487
Taking Action on Files in Event Reports . . . . .	488
Customizing Event Reports . . . . .	488
Using the Event Search Box . . . . .	488
Editing Event Reports. . . . .	491
Adding Command Line Information to Event Reports . . . . .	492
Viewing Install Event Details. . . . .	493
Viewing Event Archives. . . . .	493
Using Bit9 Alerts . . . . .	494
Creating Alerts . . . . .	498
Informational Tags for Event Alert Messages . . . . .	503
Editing Alerts . . . . .	504
Alert Priority . . . . .	504
Deleting Alerts . . . . .	505
How Alerts are Triggered. . . . .	505
Mail Notification for Triggered Alerts . . . . .	506
Reminder Mail for Triggered Alerts . . . . .	507
Manual and Automatic Alert Resets. . . . .	507
Viewing Alert Instances and History . . . . .	510
Managing Alert Email Subscriptions . . . . .	511
Detecting Agent Issues with Computer Security Alerts. . . . .	512
Criteria Triggering a Security Alert. . . . .	512
Alerts for File Prevalence. . . . .	514
Prevalence Alerts . . . . .	514
Monitoring Specific File Executions . . . . .	516
Creating a Meter from the File Details Page . . . . .	520
<b>19 Monitoring Change: Baseline Drift Reports . . . . .</b>	<b>521</b>
Baseline Drift Overview . . . . .	522
How Drift and Risk are Measured . . . . .	523
Viewing and Managing Baseline Drift Reports . . . . .	524
Viewing Baseline Drift Report Results . . . . .	525
Report Results: Computer View. . . . .	526
Report Results: File Views. . . . .	526
Drift by Files: Top-Level Files on All Computers. . . . .	528

Drift by Files: Associated Files Report . . . . .	529
Drift by Files on a Single Computer . . . . .	529
Responding to Drift Report Results . . . . .	530
Adding Drift Results to a Snapshot . . . . .	531
Creating and Editing Reports . . . . .	532
Creating a Baseline Drift Report . . . . .	533
Advanced Baseline Drift Report Options . . . . .	535
Advanced Options: File Filter Options . . . . .	535
Advanced Options: File Comparison Method . . . . .	536
Advanced Options: Report Detail Level . . . . .	537
Using Filters in Target and Baseline Definitions . . . . .	537
Drift in Multi-Platform Environments . . . . .	538
Managing Snapshots . . . . .	539
Creating and Modifying Snapshots . . . . .	539
Viewing and Editing Snapshots . . . . .	541
Managing Files in Snapshots . . . . .	542
Deleting Snapshots . . . . .	542
Displaying Baseline Drift Reports in Graphs . . . . .	542
Creating Baseline Drift Alerts . . . . .	544
<b>20 Advanced Threat Detection . . . . .</b>	<b>547</b>
Overview . . . . .	548
Indicator Sets for Threat Detection . . . . .	549
Indicator Set Details . . . . .	551
Indicator Set Exceptions . . . . .	553
Indicator Set Exception Details . . . . .	555
Updates to Indicator Sets . . . . .	557
Tracking Indicator Set Updates . . . . .	557
Monitoring Threat Reports . . . . .	558
Threat Views on the Events Page . . . . .	558
Fields in Threat-Related Events Views . . . . .	559
Reviewing Threat Event Reports . . . . .	559
Showing and Modifying View Parameters . . . . .	560
Threat Events in Syslog Output . . . . .	561
Exporting Threat Event Data to CSV Files . . . . .	562
Threat Views on the Files Pages . . . . .	562
Threat-Related Alerts . . . . .	562
Responding to Threats . . . . .	563
Responding to Threats with Event Rules . . . . .	564
<b>21 Using and Customizing Dashboards . . . . .</b>	<b>567</b>
Dashboards Overview . . . . .	568
Dashboard Elements . . . . .	570
Using Portlets . . . . .	570
Getting More Detailed Data . . . . .	571

Portlet Toolbar Buttons . . . . .	571
Collapsing, Expanding, and Exploding Portlets . . . . .	572
Entering Information into Portlets . . . . .	572
Other Portlet Controls . . . . .	573
Viewing Other Dashboards . . . . .	573
Changing Dashboard Appearance . . . . .	576
Changing Dashboard Layout . . . . .	577
Portlet Distribution in Layouts . . . . .	578
Changing Dashboard Width . . . . .	578
Changing Dashboard Background Color . . . . .	578
Moving Portlets . . . . .	578
Creating, Editing and Managing Dashboards . . . . .	579
Shared Dashboards . . . . .	580
Creating a New Dashboard . . . . .	581
Copying a Dashboard . . . . .	582
Editing a Dashboard . . . . .	583
Managing the Default Home Page . . . . .	584
Deleting a Dashboard . . . . .	584
Managing Dashboards from the Dashboards Page . . . . .	585
Creating and Customizing Portlets . . . . .	586
Portlet Types and Subtypes . . . . .	586
System Portlets . . . . .	586
Editing Portlet Details . . . . .	587
Deleting Portlets . . . . .	587
Creating Custom Portlets . . . . .	588
Using Tables in Portlets . . . . .	591
Table-only Portlets . . . . .	591
Supplemental Tables in Portlets . . . . .	594
Using Filters in Portlets . . . . .	595
Nesting Groups of Expressions . . . . .	598
<b>22 Locating Files . . . . .</b>	<b>599</b>
Find Files Overview . . . . .	600
Initiating Find Files from Other Pages . . . . .	600
Defining a Search on the Find Files Page . . . . .	601
Finding Files by Name . . . . .	601
Adding a Pathname to a File Search . . . . .	603
Finding Files by Hash . . . . .	603
Using Find Files Results . . . . .	604
Special Cases in Results . . . . .	604
Files on Offline Computers . . . . .	604
Files on Deleted Computers . . . . .	605
Deleted Files . . . . .	605
Files on Computers Still Initializing or Synchronizing . . . . .	606

Saved Views for File Searches .....	606
<b>23 System Configuration .....</b>	<b>609</b>
Overview .....	610
The General Configuration Tab .....	611
Viewing Server Status and Options .....	612
Configuring Active Directory Integration .....	614
Configuring Agent Management Privileges .....	615
Connection Status and Agent Management Choices .....	616
Event Management Options .....	617
Managing the Bit9 Event Database .....	618
Setting Limits for Event Deletion .....	618
Enabling Daily Event Archiving .....	619
Moving the Database to an External Server .....	619
Setting up External Event Logging .....	619
Logging Events to a Syslog Server .....	619
Logging Events to a Supplemental SQL Server .....	620
Securing Agent-Server Communications .....	623
Security Status .....	624
Current Certificate Details .....	624
Verifying that the Server Name and Certificate Match .....	626
Importing a Certificate .....	626
Enabling Certificate Verification .....	627
Advanced Configuration Options .....	627
Backing Up the Bit9 Server .....	631
Restoring the Bit9 Server .....	634
Configuring Alert and Approval Request Mail .....	635
Configuring Standard Email for Notifications .....	637
Configuring Secure Email for Notifications .....	638
Specifying a Global Alert Subscriber .....	639
Managing Bit9 Platform Licenses .....	640
Viewing Your Bit9 License Limits and Use .....	640
License Warnings .....	641
Adding Licenses .....	641
Confirming License Addition .....	642
Activating Bit9 SRS .....	643
Bit9 SRS Availability Status .....	645
Deactivating Bit9 SRS .....	646
Using a Proxy Server for Bit9 SRS .....	646
Bit9 SRS Synchronization .....	647
Activating Carbon Black Server Integration .....	648
Creating a Carbon Black User for the Integration .....	649
<b>24 Monitoring System Health .....</b>	<b>651</b>
Overview .....	652

Enabling System Health Indicators . . . . .	653
Disabling System Health Indicators . . . . .	653
Viewing the System Health Page . . . . .	654
Navigating on the System Health Page . . . . .	655
Health Indicator State . . . . .	656
System Health Alerts . . . . .	657
System Health Events . . . . .	658
<b>A Live Inventory SDK: Database Views . . . . .</b>	<b>659</b>
Performance Considerations . . . . .	659
Upgrading from a Previous Version . . . . .	659
Schema Overview: bit9_public . . . . .	661
Specifying a Schema User . . . . .	661
Schema Views and Diagram . . . . .	661
Schema Diagram for bit9_public . . . . .	663
Details of Database Views . . . . .	665
ExComputers . . . . .	665
ExInfo . . . . .	667
ExMeters . . . . .	668
ExEvents . . . . .	669
ExFileCatalog . . . . .	670
ExFileInstances . . . . .	673
ExDeletedFileInstances . . . . .	675
ExFileInstanceGroups . . . . .	676
ExApprovalRequests . . . . .	677
Sample Queries . . . . .	679
<b>B Bit9 API . . . . .</b>	<b>683</b>
Overview . . . . .	684
API Authentication and Access Control . . . . .	684
Available Objects . . . . .	685
Using the Bit9 API to Add a Connector . . . . .	686
<b>C Bit9 Connector for Network Security Devices . . . . .</b>	<b>687</b>
Overview . . . . .	688
Preparing to use the Connector . . . . .	689
Enabling Microsoft SCEP Integration . . . . .	689
SCEP Hash Identification Limitations . . . . .	691
Enabling Palo Alto Networks Integration . . . . .	692
Integrating Palo Alto Networks Appliances for Notifications . . . . .	692
Palo Alto Networks Notification Appliance Status in Bit9 . . . . .	695
Modifying or Deleting an Appliance Integration . . . . .	695
Integrating with the WildFire Cloud for Analysis . . . . .	696
Integrating with the WildFire Public Cloud . . . . .	696
WildFire Public Cloud Query Limits . . . . .	697
Integrating with a WildFire Private Cloud Device . . . . .	697



Enabling Check Point Integration . . . . .	698
Integrating Check Point Log Servers with Bit9 . . . . .	699
Custom Import Filters for Check Point . . . . .	703
. . . . . Check Point Log Server Status in Bit9	705
Modifying or Deleting a Log Server Integration . . . . .	706
Integrating with Check Point for File Analysis . . . . .	707
Connecting to a Threat Emulation Appliance . . . . .	707
Connecting to the ThreatCloud Emulation Service . . . . .	708
ThreatCloud Emulation Lookup Limits. . . . .	708
Enabling Automatic Threat Emulation Lookups . . . . .	709
Enabling FireEye Integration . . . . .	709
Performance and Bandwidth Considerations . . . . .	709
Integrating with FireEye Notifications . . . . .	709
Integrating with FireEye for Analysis . . . . .	712
FireEye Threat Level Mapping . . . . .	715
Default Threat Level Mapping Rule . . . . .	716
Adding or Editing Threat Level Mappings . . . . .	716
Limiting Notifications to Mapped Threats . . . . .	717
FireEye Appliance Status in Bit9 . . . . .	717
Enabling Console Account Permissions . . . . .	718
External Notifications . . . . .	718
Action Menu on External Notifications Table Page . . . . .	722
Saved Views on the Notifications Table Page . . . . .	722
Notification Table Access from File Details Pages . . . . .	723
Choosing Correlation Level for External Notifications . . . . .	723
Notifications from Multiple Analysis Environments . . . . .	724
External Notification Details . . . . .	725
Total Files Tab . . . . .	726
Known Files Tab . . . . .	727
Files On Computers Tab . . . . .	727
Directories Tab . . . . .	727
Registry Keys . . . . .	728
More Details Tab . . . . .	729
History Tab . . . . .	729
Showing Related Notifications . . . . .	729
Showing XML Details . . . . .	730
External Console Access . . . . .	730
Getting Malware Details . . . . .	730
Managing Notification Status . . . . .	730
Banning Externally Reported Malware . . . . .	732
Manually Banning Files . . . . .	732
Special Rules for Reporting or Banning Malware . . . . .	733
Registry Rules . . . . .	733
Custom Rules for Directory Control . . . . .	733

Analysis of Suspicious Files on Endpoints . . . . .	734
Monitoring Files Submitted for Analysis . . . . .	735
Analysis Status . . . . .	737
Actions on the Analyzed Files tab . . . . .	737
Bit9 Logging of Connector-related Events . . . . .	738
Additional Log Information . . . . .	740
<b>D Diagnostic Files . . . . .</b>	<b>741</b>
Overview . . . . .	742
Uploading Agent Diagnostic Files . . . . .	742
Canceling or Retrying an Upload . . . . .	743
Viewing Diagnostic Files . . . . .	743
Deleting Uploaded Diagnostic Files . . . . .	745
<b>E Uploading Files from Agents . . . . .</b>	<b>747</b>
Overview . . . . .	748
Enabling Access to File Upload Features . . . . .	748
Scheduling Uploads . . . . .	749
Starting Uploads of Inventoried Files from Tables . . . . .	749
Starting Uploads from the File Instance Details Page . . . . .	750
Starting Uploads by Path from the Computer Details Page . . . . .	751
Viewing the Uploads Table . . . . .	752
Diagnostic Files . . . . .	754
Downloading Uploaded Files . . . . .	755
Upload Configuration Options . . . . .	755
Deleting Uploaded Files . . . . .	755
Changing the Uploaded File Location . . . . .	756
<b>F Exporting Bit9 Data for External Analysis . . . . .</b>	<b>759</b>
Overview . . . . .	760
Preparing to Use External Analytics . . . . .	760
Data Format and Management . . . . .	761
Data Volume for Exported Analytics . . . . .	762
Limiting Export Directory Size . . . . .	762
Local vs. Network Log Files . . . . .	762
Enabling External Analytics in the Bit9 Console . . . . .	763
Editing or Disabling the External Analytics Integration . . . . .	766
Adding a Custom Rule to Ignore Analytics Log Files . . . . .	767
Enabling an External Tool for Bit9 Data Analytics . . . . .	767
Enabling Splunk to Collect Bit9 Data . . . . .	768
Configuring the Splunk Server for Bit9 Access . . . . .	768
Installing the Splunk Forwarder and App on the Bit9 Server . . . . .	769
Viewing Bit9 Data in External Analytics Tools . . . . .	770
Linking to an External Tool from the Bit9 Console . . . . .	770
Using the Splunk App for Bit9 Security Platform . . . . .	771
Dashboards in the Splunk App for Bit9 . . . . .	771

Field Mappings to CIM in the Splunk App for Bit9 ..... 777

**Index .....779**



## Chapter 1

# Bit9 Security Platform Overview

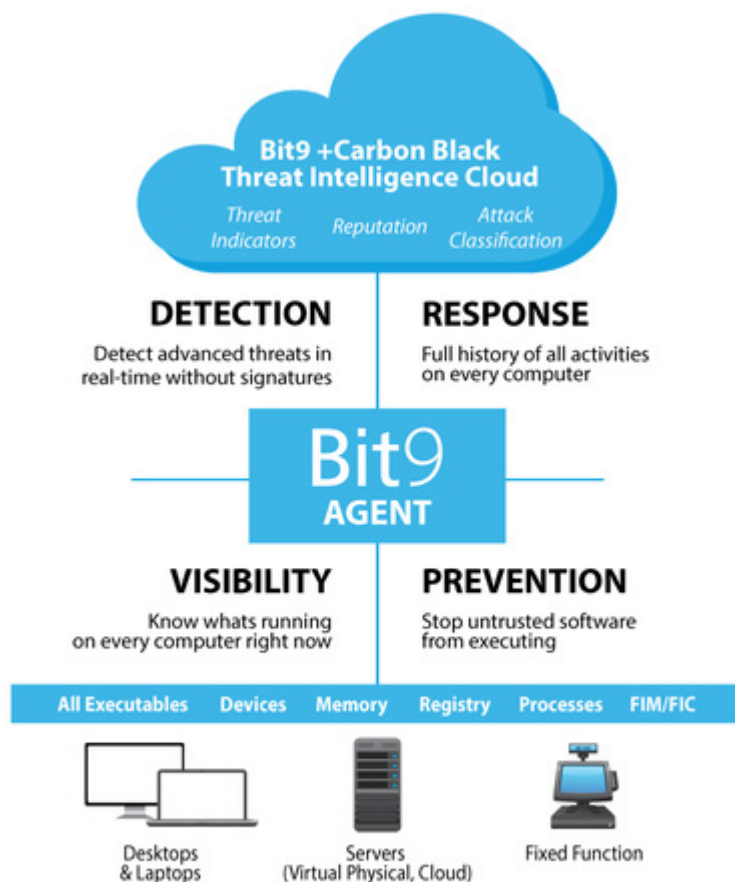
This chapter introduces the Bit9 Security Platform, explains key concepts, and suggests operating strategies for preventing unauthorized or malicious file execution on your endpoints.

### Sections

Topic	Page
<a href="#">What is the Bit9 Security Platform?</a>	34
<a href="#">How the Bit9 Security Platform Works</a>	38
<a href="#">System Architecture</a>	39
<a href="#">File State, Whitelisting and Blacklisting</a>	41
<a href="#">Security Policies and Levels</a>	43
<a href="#">Operating Strategies</a>	45

## What is the Bit9 Security Platform?

The Bit9 Security Platform is the a comprehensive endpoint threat protection solution and widely deployed whitelisting product. Combining a trust-based and policy-driven approach to application control with real-time threat intelligence, Bit9 continuously monitors and records all endpoint and server activity to prevent, detect and respond to cyber-threats that evade traditional security defenses. With open APIs and a broad partner ecosystem, Bit9 provides exceptional flexibility to seamlessly integrate with both in-house and third-party tools.



**Instant Visibility** – Once installed, the Bit9 agent provides administrators with real-time visibility into all executable-type files running across their environment. Working with the Bit9 Threat Intelligence Cloud, the Bit9 agent provides administrators with trust ratings and actionable intelligence to easily identify and automatically take action against those files most likely to be malicious.

**Prevention with Flexibility** – With the Bit9 Security Platform, administrators can stop attacks before they occur. Leveraging Bit9's proactive "Default-Deny", "Detect-and-Deny" or "Detonate-Deny" prevention capabilities, the Bit9 Security Platform can dramatically reduce an organization's attack surface while providing administrators with the flexibility they need to ensure the right balance between protection and access.

**Advanced Detection** – The Bit9 Security Platform includes powerful automated and cloud delivered advanced threat detection technologies to quickly identify and stop attacks. Leveraging Advanced Threat Indicators from the Bit9 + Carbon Black Threat

Intelligence Cloud, Bit9 continuously monitors and examines endpoints to identify potential patterns of compromise and detect malicious activity across every endpoint device in an organization's environment.

By using real-time endpoint data, Bit9's advanced threat indicators go beyond "indicators of compromise" by combining endpoint activity, cloud delivered threat intelligence, and heuristics to identify threats based on patterns rather than single event-based indicators of compromise. This combination of detection mechanisms enables Bit9 to reduce the number of false positive alerts and detect threats both at initiation and while they are in progress, unlike poll-based detection methods which can only detect compromise after it has occurred.

**Rapid Response** – Once an attack is detected, Bit9 provides a variety of tools to help you rapidly respond, log and investigate security incidents. Bit9's unique "Detect-and-Deny" protection capabilities enable administrators to quickly respond to malicious activities by terminating active processes and immediately banning any future execution of the attack in your environment. Additionally, Bit9's full historical record of endpoint activity quickly provides administrators with a full impact assessment of where malware has executed, where it started, how it spread, and ultimately what systems were impacted and what actions or data, if any, was taken.

**Open API Architecture** – Bit9's open architecture helps organizations integrate with the entire security stack to automate and simplify the security process. Through Bit9's RESTful API and broad partner integration ecosystem, the Bit9 Security Platform provides organizations with unmatched openness and extensibility to integrate their security solutions for improved automation, reporting and faster security response times, via third-party security products (SIEM, Network, Endpoint, Operations) or custom in-house tools.

Using the Bit9 Security Platform, you can:

- Stop malicious software by blocking known viruses, trojans, application exploits, and custom and targeted attacks
- Stop zero-day threats by allowing only approved software to run
- Create rules to monitor and control access to the Windows registry
- Create memory rules to monitor and control access to specific processes on Windows computers
- Create file integrity monitoring and control rules to prevent or report access to critical, non-executable system configuration files
- Reduce the burden of compliance through streamlined audits, activity monitoring, violation notification, and policy enforcement
- Use the Bit9 Software Reputation Service (SRS) to identify and classify the risk associated with the software discovered in your environment using reputation services, and to automatically approve files or publishers considered trusted by Bit9 + Carbon Black Threat Intelligence Cloud
- Prevent data theft and leakage by auditing and controlling the transfer of sensitive data to attached storage devices on Windows computers
- Create rules to approve or ban file execution on storage devices by model or serial number on Windows computers
- Monitor drift away from a baseline of files to minimize risk, identify needed remediations, maintain compliance, and reduce support costs

- Monitor threats using advanced threat indicators, Bit9 events, file details, and alerts.
- Automate file- and computer-related actions based on incoming events.
- Use the Bit9 OpenAPI to integrate third-party network, endpoint, SIEM, and analytic security products and services with the Bit9 Server for notifications and analysis.
- Export Bit9 data for use by external analytics products such as Splunk.

Table 1 shows complementary Bit9 features that provide visibility into what files are on your computers, give you control of unauthorized software and hardware, and allow flexible management of computers at your site:

**Table 1:** Bit9 Security Platform Features

Feature	Description
<b>Live File Inventory and Baseline Drift Tracking</b>	The Bit9 Security Platform can track all files of interest on all computers all the time. This near-real-time inventory means that the Bit9 Security Platform can provide a wide variety of information about these files, and about the rate and nature of change across your organization. One benefit of this information is Baseline Drift Reports, which report changes in the file inventory on one or more computers. Another is the ability to locate all instances of a specified executable file that exist on managed computers.
<b>Bit9 Software Reputation Service (SRS) File Identification &amp; Reputation Services</b>	Bit9 Software Reputation Service (SRS) identifies and classifies files. It assigns a <b>Trust Factor</b> to files based on a variety of sources, including the source of the file, its prevalence on computers running the Bit9 Agent, results of anti-virus scanning, and whether it has a legitimate digital certificate. You can automatically approve files or publishers that meet a certain trust threshold.
<b>Event Tracking</b>	The Bit9 Security Platform keeps an up-to-date database of file-related events, as well as other activities involving the Bit9 Server or managed computers. From this data, you can view predefined or custom reports that can give visibility into changes to your environment and significant Bit9 Server operations. You also can trigger alerts based on certain events. Bit9 events can be exported to Syslog for integration with SIEM systems, to data analytics systems, and to CSV files.
<b>Modes</b>	Active Bit9 Agents can be operated in one of two modes: <b>Visibility mode</b> provides the file and event tracking features of the Bit9 Security Platform, but does not enforce file or device bans or other security restrictions. <b>Control</b> mode blocks banned files and allows you to choose one of three Enforcement Levels to determine how unapproved files (i.e., files neither approved nor banned) are treated. Control policies can be configured to enforce other file and device security rules.



Feature	Description
<b>Enforcement Levels and Policies</b>	<p>Enforcement Levels and policies work in combination to control file and device activity on specific computers. Depending upon the Enforcement Level you choose, execution of banned files as well as unapproved (neither approved nor banned) files can be blocked. Enforcement Levels range from very restrictive to no enforcement.</p> <p>Policies are rule sets that include an Enforcement Level and other settings, such as the ability to block or control the behavior of some removable devices on Windows computers. All computers managed by the Bit9 Security Platform have an assigned policy.</p>
<b>Flexible and Emergency Lockdown</b>	<p>You can run different groups of computers at different security levels. For example, you may choose to run some computers at High Enforcement Level, which prevents computers from executing unapproved files that were not present when the Bit9 Agent was installed, while allowing other computers greater privileges.</p> <p>If necessary, you can implement an emergency lockdown to move all computers to High Enforcement during attacks or high threat periods. You can return the systems to their previous security level when you believe the threat is contained.</p>
<b>File Integrity Monitoring and Control</b>	<p>The Bit9 Security Platform allows you to create custom software rules that apply to specified files or paths. These include File Integrity rules, with which you can monitor, and if you choose, restrict modifications to a specific folder or folders matching your specification.</p>
<b>Software Rules: Bans</b>	<p>Bans enable you to specify files (by name or hash) to be blocked for some or all computers at your site. You can ban files individually, and also can ban all files identified on a list of hashes you provide. You also can ban all files from a specified publisher.</p>
<b>Software Rules: Approvals</b>	<p>Several complementary software approval methods enable you to approve legitimate software to run on all computers, on groups of computers (i.e., by policy) or to <i>locally</i> approve software to run on a single computer. You can integrate approval rules with Bit9 Software Reputation Service (SRS) to automatically approve files meeting a specific Trust level according to analysis by the service.</p>
<b>Registry Rules</b>	<p>You can specify rules to protect specific registry key/value patterns from alteration on Windows computers.</p>
<b>Memory Rules</b>	<p>You can specify rules to protect a process from access or alteration by any (or specified) other process(es) or user(s) on Windows computers.</p>
<b>Device Rules: Approvals and Bans</b>	<p>You can approve or ban file execution and writing on detected storage devices on Windows computers. You can approve and ban device models or specific, individual devices, and you can apply the rules to some or all computers.</p>
<b>Notifiers and User-Initiated Approval Requests</b>	<p>When a Bit9 rule blocks file access, you can display a notifier that explains the block to the user. The notifier can provide an optional file approval request method that lets you track and respond to requests directly in the Bit9 Console.</p>

Feature	Description
<b>Detection: Advanced Threat Indicators</b>	You can enable advanced threat indicators that will trigger events when suspicious conditions occur, and you can fine-tune these indicators by creating exceptions for events that you consider benign.
<b>Event-Triggered Actions</b>	You can create Event Rules that specify an action to be performed when a file- or computer-related event occurs that matches filters you define. You also can create an alert that reports when a specified event rule is triggered.
<b>Integration with Network Security Devices</b>	You can integrate the Bit9 Server with one or more network security devices or services from third-parties, including Check Point, Palo Alto Networks, FireEye and Microsoft EMET.
<b>Access via the Bit9 API</b>	You can use the RESTful API for the Bit9 Platform to write code to interact with Bit9 Platform via custom scripts or from other applications. API code can be consumed over the HTTPS protocol using any language that can create get URI requests, post/put JSON requests, and interpret JSON responses.
<b>Integration with External Data Analyzers</b>	You can export Bit9 events, file operations data, and file catalog data for use by external analytics products such as Splunk.
<b>System Health Monitoring</b>	You can opt in to System Health indicators that monitor and report on factors affecting the operation of this Bit9 Server, such as compliance with the operating environment requirements.

## How the Bit9 Security Platform Works

The Bit9 Security Platform tracks executable files and monitors their prevalence and execution. *Initialization*, the inventory of files by Bit9, begins immediately after installation of the Bit9 Agent on a computer. Each file found on a computer during the initial inventory is *locally approved* on that computer unless it has been already banned on the Bit9 Server. Local approval does not change the global state of a file.

After initialization, new unidentified files that appear on computers managed by Bit9 are classified as having a state of *Unapproved*, both globally and locally, on the computer on which they were found. A file keeps its *Unapproved* state until it becomes *Approved* or *Banned*. Once a file has been approved, it is allowed to execute but continues to be tracked.

The Bit9 Security Platform features several automatic file approval methods (trusted directories, approved publishers, trusted users, pre-configured updaters for Windows computers, reputation approvals, and bulk approval of files from a list of hashes) that make it easy to approve new software without having to do it file-by-file. You also can manually mark individual files as approved or banned.

Other Bit9 features monitor activity on your computers, which might help you decide on what files to approve or ban. The Bit9 Server can tell you:

- Whether a file exists on your computers
- Which computers have the file
- Where and when the file first arrived in your environment

- What is known about the source, category, trust level, and threat of the file
- Whether and when a file has executed, and on which computers
- Whether a file has propagated and, if so, whether it has been renamed
- On Windows computers, whether attached storage devices (including USB, SCSI, and others) exist on your network, when they first were discovered, and on what computer
- How the inventory of files on computers has changed over time

## Files Tracked by the Bit9 Security Platform

In the Bit9 Console and throughout this manual, you will often see the term “files.” What constitutes a “file” depends upon the Bit9 feature:

- For Bit9’s live inventory, a “file” is an *executable* or *script* file. When you install the Bit9 Agent on a computer, it analyzes all files on the system, determines which of them are executables or scripts, and keeps an inventory of these files. Non-executable files are ignored once they are identified.  
The Bit9 Security Platform determines that a file is an executable by the content of the file, not its file extension. The Bit9 Security Platform determines that a file is a script by a combination of factors, and users can add to or modify these script definitions. Only executable and script files can be approved or banned. Certain configuration settings can exclude special cases of these files from tracking and inventory.
- For File Integrity Monitoring, access to *non-executable data and configuration files* can be tracked if you register the files with the Bit9 Security Platform through a File Integrity Control rule. Once a file or path is covered by such a rule, any attempt to access it generates an auditable event in the Bit9 Security Platform, and if you choose, the attempt is blocked.

## System Architecture

The Bit9 Security Platform architecture consists of the following components:

- Bit9 Server software provides central file security management, event monitoring, and a live inventory of files of interest on all agent systems.
- Bit9 Agent software runs on servers, desktops, laptops, virtual machines and fixed-function devices. It monitors files and either blocks or permits their execution based on security policy settings. It also reports new executable and script files to the Bit9 Server and enforces other rules you configure.
- Bit9 Software Reputation Service (SRS) compares new files introduced on computers running the Bit9 Agent to a database of known files, providing information on threat level, trust factor, and software categorization. If you choose, you can use trust information to automatically approve files.
- Bit9 also may be integrated with third-party products. This includes external analytics products such as Splunk and network security products such as those from Check Point, FireEye, and Palo Alto Networks.

## Bit9 Server

Bit9 Server software runs on standard Windows computers. It can be run on a dedicated system or as a virtual machine. The Bit9 Server manages policies and rules, including software and device approvals and bans, and provides visibility into events and file activity on computers running Bit9 Agents. The Bit9 Console, a convenient web-based user interface, provides access to the Bit9 Server from any connected computer.

The Bit9 Server database uses SQL Server, either on the same machine as Bit9 Server or on separate hardware. Key Bit9 Security Platform data is accessible outside of Bit9 Security Platform through a series of published views in the database that are part of the Live Inventory SDK. Bit9 Security Platform events also can be output to a Syslog server or data analytics system for further analysis.

## Integrating Bit9 Security Platform with Active Directory

You may have already defined and named users, computers, and groups by using Microsoft Active Directory. Bit9 Server can take advantage of your Active Directory environment to set access privileges for users of the Bit9 Console, assign security policies to computers, provide user and computer metadata, and designate certain groups or users to be able to install software (and have it automatically approved) on Bit9 Security Platform-managed computers.

## Bit9 Agent

Bit9 Agent software runs on client computers. It monitors file and process activity and communicates with the Bit9 Server when necessary. On Windows computers, it also monitors connected storage devices and registry activity. Even when disconnected from the server, the agent continues to enforce the last specified bans and security policies it received. When a disconnected computer running the Bit9 Agent reconnects, the agent receives policy and rule updates from the server and communicates relevant file activity that occurred during the time it was off the network.

The Bit9 Agent runs silently in the background until it blocks a file, at which point it can display a message to the computer user, explaining why the file was not permitted to execute. Depending on the file state, the agent's security level, and other configuration choices, Bit9 Security Platform may also let the user on the client computer choose to run a blocked file. You also can enable mechanisms for users to request approval of blocked files, either informally via email or using a formal request process built into and tracked by the Bit9 Security Platform.

## Trust Rating from Bit9 Software Reputation Service

Bit9 Software Reputation Service (SRS) is a web service, hosted by Bit9, that helps identify and classify software discovered on your computers by comparing it to an extensive database of known files. Based on weighted analysis, Bit9 SRS further assigns a threat level (malicious, potentially malicious, unknown, or clean) and a trust rating (0-10 or unknown) to each file. The Bit9 Server can include this information in its live file inventory so that you immediately know the threat status and other key information about files on your systems. If you have Bit9 SRS enabled, you can “analyze” any file in the Bit9 Server inventory to get whatever information is available.

A file's trust rating goes beyond the information available from one anti-virus scan. It is based on a series of factors, including how long and on how many computers the file has

been seen, whether it has a trusted digital certificate, and the results of scanning by multiple anti-virus programs.

For example, a file that scans as clean on anti-virus programs, has a trusted digital certificate from a known publisher, and appears on many computers for a long period of time might have a Bit9 trust rating of 10, highly trusted. Another file that also produces clean anti-virus scans but has only recently been seen, is on very few computers, and does not have a digital certificate might only get a trust rating of 2, low trust.

You can use the trust rating provided by Bit9 SRS to automatically approve files, either based on their own trust rating or the rating of their publisher. By using Reputation Approvals, administrators can enforce their chosen security posture as it relates to file or publisher trust level and approve high trust software with no administrative overhead.

## File State, Whitelisting and Blacklisting

Several key feature groups work together in the Bit9 Security Platform to secure computers on your network. At the heart of this security capability is the ability to classify files according to their *state*. Groups of security rules, called policies, control how different groups of computers treat files in different states. This section describes the primary file states – approved (whitelisted), banned (blacklisted), and unapproved – and how they can be changed.

### Global State

The Bit9 Server maintains a central database of unique files (determined by hash) for all executable files tracked on computers running the Bit9 Agent. You can view the *global state* of these files in the File Catalog. Global state determines what the file is allowed to do on agent-managed computers with different Enforcement Levels.

Global state is a combination of:

- *File State*, which indicates the approval/ban state of the file itself, and
- *Publisher State*, which is the approval state of the file's publisher (if known).

A file can have a global state of:

- *Approved* – for all computers
- *Approved by Policy* – approved for some computers, unapproved for others
- *Banned* – for all computers
- *Banned by Policy* – banned for some computers, unapproved for others
- *Unapproved* – for all computers
- *Mixed* – banned for some computers but approved for others

Global State cannot be modified directly, but can be modified by changing the *file state* or *publisher state*. Bit9 Security Platform provides a variety of ways to modify the file state. See [Chapter 8, “Approving and Banning Software,”](#) for details. [Chapter 7, “File and Publisher Information,”](#) shows additional details for files tracked by the Bit9 Security Platform.

## Local State

While the Bit9 Server keeps a global state for a file, each *instance* of a file on a computer running the Bit9 Agent has its own *Local State*, which indicates what the file is allowed to do on the computer it was found on, depending upon its Enforcement Level.

Files with a Global State of Unapproved may have different local states. In particular, you can locally approve a file by various methods, as long as that file was not globally banned. The Bit9 Security Platform includes local file state information in its Files on Computers inventory of all tracked file instances.

A file can have a local state of:

- *Approved*
- *Banned*
- *Unapproved*
- *Deleted* (the file has been deleted recently and will be removed from the database on next update)

In addition to its primary state, each file instance has Local File Details (see [Chapter 7, “File and Publisher Information”](#)) that may identify the source of its approval or other decisions made about it in the Bit9 Security Platform. These details are primarily use by Bit9 Support.

## File Approval Methods

Software approval ensures that users of computers running the Bit9 Agent can freely install and run known-good applications regardless of the Bit9 Security Platform settings and Enforcement Level in effect. Approving files, often called “whitelisting,” also can reduce time devoted to tracking files you are not concerned about. The Bit9 Security Platform supports several complementary methods for approving software on computers:

- When you need to pre-approve applications to run on all computers, you can designate trusted directories, publishers, or updaters to automatically generate approvals.
- When you want to protect against advanced threats and would like to reduce the number of files you need to approve individually, you can enable automatic reputation approvals of files based on file or publisher trust in Bit9 Software Reputation Service (SRS).
- You can approve an individual file by hash, either for all computers or by policy. In addition, you can create multiple individual file approvals by importing a list of file hashes you want to approve.
- When you need to approve software for installation on selected individual computers, either designate trusted users (or groups) to perform installations, or choose one of the Bit9 Security Platform’s local approval methods.

See [“What is Bit9 Software Approval?”](#) on page 224 for more details.

## File Ban Methods

In Control mode, the Bit9 Security Platform lets you ban specific files from executing on all computers, or on computers associated with specified policies. Banning files is often called “blacklisting.” You can ban files using the following methods:

- *File-name bans* are platform-specific (Windows, Mac, Linux). For the named platform, they ban execution of named files on either *all* systems on running the Bit9 Agent or on all systems in policies you specify.
- *Hash bans* prevent files matching a unique hash from executing regardless of the file name used. They are enforced for all platforms, either on all systems running the Bit9 Agent or on systems in policies you specify. You can ban more than one file in a single operation by importing a list of hashes.
- *Publisher bans* prevent files identified as being from a specified publisher from executing. They are enforced either on all Windows systems running the Bit9 Agent or on systems in policies you specify.

See [“What are Bit9 Software Bans?”](#) in [Chapter 8, “Approving and Banning Software,”](#) for more details.

## Custom Rules

In addition to the variety of ban and approval rules described above, the Bit9 Security Platform provides other ways to protect your computers, allow needed software to run, and optimize performance.

Custom Rules allow you to designate one or more paths, either at the directory or the file level, at which certain activities are allowed or blocked. In some cases this involves changing the state of files, but in others it simply allows, blocks, or disables certain behavior on a case-by-case basis without any global rule changes. You can use Custom Rules for File Integrity Control, to create a Trusted Path for your installation directories, to reduce tracking of files in directories known to be safe or not of interest, and for many other purposes you can configure.

See [Chapter 12, “Custom Software Rules,”](#) for more details.

## Security Policies and Levels

Bit9 Security Platform policies are named groups of protection rules shared by targeted groups of computers running the Bit9 Agent – every computer running a Bit9 Agent must belong to a policy. You create policies based on your security and organizational requirements. For example, you might base policy membership on functional group (e.g., marketing, customer service, IT); location; or type of computer (e.g., laptop, desktop, server).

Each policy has its own Bit9 Agent installer, which is automatically generated on the server when you create the policy. Each installer automatically assigns a policy to each agent it installs. However, if you choose, you can have the Bit9 Server assign a policy based on Active Directory data for the user and/or computer running the agent each time the computer with the Bit9 Agent connects to the server.

See [Chapter 5, “Creating and Configuring Policies”](#) for details on policies.

## Policy Settings

Policy settings define the way you want the Bit9 Security Platform to manage a particular group of computers. There are three categories of settings:

- *Basic Policy Definitions* – These include the policy name and other descriptive information, whether computers in this policy allow agent upgrades, whether live file inventory is activated for these computers, and the basic security level (the Mode and Enforcement Level) for the policy. Modes and Enforcement Levels are described in more detail below.
- *Device Settings* – Device settings control the way a Bit9 Security Platform policy treats removable devices on Windows computers. You can make different rules to control read, write, and execute operations on devices, and you can specify that approved and banned devices are treated differently than devices that have not been classified.
- *Advanced Settings* – Advanced policy settings primarily control whether computers in a policy have certain file types blocked. The possible values are Active, Off, and Report Only.

See [Chapter 5, “Creating and Configuring Policies”](#) for full details on policy settings.

## Modes and Enforcement Levels

The Enforcement Level in a security policy controls whether unapproved files (applications that may be unidentified and that have not been approved or banned) are allowed to execute. The availability of different Enforcement Levels enables you to choose a setting for each policy that suits the security and user requirements for the group of computers associated with that policy.

Bit9 Security Platform offers three different modes of operation: Agent Disabled, Visibility, and Control. Disabled agents neither enforce rules on nor report information from their computers. Agents in Visibility mode collect and report information but do not enforce rules.

Control mode offers the full range of Bit9 Security Platform features, including tracking of files and device activities, and enforcement of bans and other rules that protect your computers. If a file has been banned, it is blocked at *all* Enforcement Levels in Control mode. Control mode Enforcement Levels differ primarily in how they treat unapproved files:

- *High (Block Unapproved)* – Only approved files are allowed to execute.
- *Medium (Prompt Unapproved)* – Approved files are allowed to execute. Attempts to execute Unapproved files cause a notifier dialog to display, in which the user can decide whether to Allow or Block them.
- *Low (Monitor Unapproved)* – Approved and Unapproved files are allowed to execute without prompting. The activity of these files is still monitored by the Bit9 Security Platform.

In some cases, a computer can have different Enforcement Levels when it is connected vs. when it is disconnected.



## Bit9 Security Platform Licensing and Modes

Bit9 Server can be licensed at two feature levels that parallel the available Modes described in the previous section:

- *Visibility* – This provides all of the Bit9 Security Platform’s file and event tracking and reporting capabilities, but not control features such as file and device blocking.
- *Suite* – This provides the Visibility and Control features of the Bit9 Security Platform.

License keys determine the number of agents allowed to run in each mode. You can mix licenses on the same server, having, for example, 20 Visibility licenses and 20 Suite licenses. In addition, you can purchase the upgrade at any time to bring Visibility licenses up to Suite level. Keep in mind that if you have *no* Suite licenses, Control features are not available and certain elements of the Bit9 Console documented in this manual will not appear.

See “[Managing Bit9 Platform Licenses](#)” on page 640 for information for more information on how licenses work in the Bit9 Security Platform.

## Operating Strategies

Your overall Bit9 Security Platform operating strategy depends on whether you are only interested in getting *visibility* into file activity on your network or whether you need to exercise a degree of *control* over the use of software and devices. It also could vary according to whether you want all of your computers operating at the same security level or you need to control some more than others. In addition, your strategy might change over time, perhaps due to greater experience with the Bit9 Security Platform, different threat levels, or the frequency with which your privileged users need to run new software that is not managed by IT.

Different operating strategies will require different amounts of preparation and maintenance. You might want to create a reference system – one computer that has all of the applications you want to approve for all of your users and has no applications you don’t want executed on your users’ computers. You can use this system to create a baseline for analyzing any drift of files on other computers, or over time.

Your Bit9 Technical Support or Services representative can help you develop an operating strategy appropriate for your environment.



## Chapter 2

# Using the Bit9 Console

This chapter covers the basics of using the Bit9 Console: how to log in and out, how to navigate in the user interface from the Home page and menu system, and how to view the information the Bit9 Security Platform makes available to you through tables, details pages, and dashboards. Mastering the information and tasks in this chapter will give you a head start on all other Bit9 Security Platform activities described in this guide.

### Sections

Topic	Page
<a href="#">Logging In</a>	48
<a href="#">Logging Out</a>	49
<a href="#">The Home Page</a>	50
<a href="#">Using the Main Menu</a>	53
<a href="#">Left Navigation Menu and Breadcrumbs</a>	57
<a href="#">Bit9 Console Tables</a>	58
<a href="#">Details Pages and Object Previews</a>	68
<a href="#">Menus on Details Pages</a>	69
<a href="#">Setting Preferences for Console Users</a>	71
<a href="#">Using Context-Sensitive Help</a>	73

## Logging In

The Bit9 Security Platform uses a browser-based user interface called the *Bit9 Console*. You can log in to the console from a web browser on any computer with access to your server, including the Bit9 Server itself. Although other browsers with HTML frame support should work, these Bit9-certified browsers are recommended:

- Microsoft Internet Explorer Version 10.0 or higher
- Latest Mozilla Firefox release
- Latest Chrome release
- Latest Safari version (on OS X only)

In Internet Explorer, you may need to adjust your overall security settings or set the Bit9 Console address to be part of your Local Intranet or Trusted Sites zone in order to access the Bit9 Console. The security settings are accessed by choosing **Tools > Internet Options** in Internet Explorer and clicking on the **Security** tab.

### To log in to the Bit9 Console:

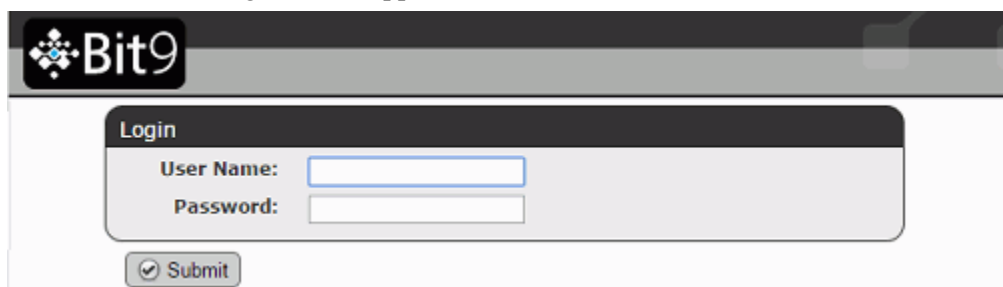
1. From any supported web browser, enter the Bit9 Server name you chose during installation, usually the server's fully qualified domain name or a configured alias:  
`https://server_name.domain.extension`
2. If you see a certificate dialog, accept the digital certificate presented for the server. A certificate is required by the web server to support SSL and HTTPS connections.
  - a. If you provided one at installation time, your company's certificate appears. Otherwise, you see a self-signed certificate created during server installation. You can accept the Bit9 certificate without compromising security.
  - b. If your browser displays a warning about the certificate, you can safely ignore the warning and click through the remaining confirmation screens.

### Note

To avoid future certificate warnings:

- In Firefox, accept the certificate permanently.
- In Internet Explorer, click through the warning, click the Certificate Error button in the IE toolbar, and install the self-signed certificate.
- In Safari, click **Show Certificate** on the warning and check the *Always trust...* box for the Bit9 Console certificate, and click **Continue**.

The Bit9 Console login screen appears:



The screenshot shows a web browser window displaying the Bit9 Console login page. At the top, there is a dark header with the Bit9 logo on the left and some navigation icons on the right. Below the header, the main content area is white. A 'Login' form is centered on the page. The form has a dark title bar with the word 'Login' in white. Below the title bar, there are two input fields: 'User Name:' and 'Password:'. Below the input fields, there is a 'Submit' button with a checkmark icon.

3. Enter your user name and password. For first-time login, enter the default user name (**admin**) and password (**admin**). For security, change the default password according to the instructions in “[Changing Passwords and Other Account Details](#)” on page 85.
4. Click the **Submit** button.
5. The Bit9 Console Home page appears. The first time any user logs in to the Bit9 Console after installation, there may be a noticeable delay in display of the Home Page. Subsequent logins will be faster for all users.

## Login, Server, Version and Alert Information

The top right corner of Bit9 Console pages shows the following information:

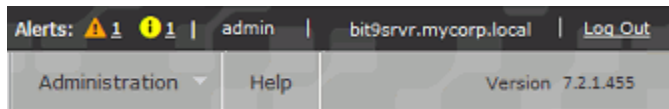
- the name of the currently logged in console user
- the name (or in some cases, the IP address) of the Bit9 Server
- the version number of the Bit9 software you are running.
- the number of Bit9 Security Platform alerts currently triggered (if any) in each of three categories with separate color symbols: High (red), Medium (orange) and Low (yellow); hovering over the symbol or number shows the alert name if there is a single alert in that category or the alert level if there are multiple alerts

## Logging Out

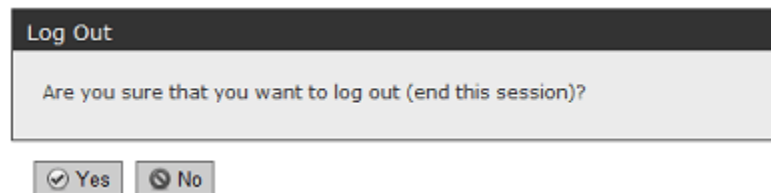
On every page of the Bit9 Console, a Logout link appears in the upper right banner area of the web page. Logging out ends your Bit9 Console session.

**To log out of the Bit9 Console:**

1. From the console banner, click the **Log Out** link:



2. Respond to the confirmation prompt:



### Important

The console user interface is documented based on users having full permissions. Features available to a specific user depend upon that user’s account privileges. Any permissions that are turned off will remove related user interface elements. Consider making users with restricted permissions aware of this so that they are not confused by the absence of features described in the Bit9 Security Platform help. See [Chapter 3, “Managing Console Login Accounts”](#) for details.

## The Home Page

The Home Page provides quick access to common tasks and information. When you log in for the first time, the Bit9 Security Platform Home page appears, with the Bit9 Console main menu at the top of the window:

The screenshot displays the Bit9 Security Platform Home Page. At the top, there is a navigation bar with the Bit9 logo and menu items: Home, Reports, Assets, Rules, Tools, Administration, and Help. The user is logged in as 'admin' on 'bit9srvr.mycorp.local'. The main content area is divided into several sections:

- Alerts:** A table showing a 'Backup Missed Alert' of type 'System Alert', enabled, and modified on 2012-10-06 08:24:22.
- Top X:** Search filters for top items, including 'Find top: 10', 'Blocks by Computer', and 'Max age: Last Day'.
- Find Computer:** Search by 'Computer name or IP' or 'User name'.
- Find Files or Events:** Search by 'Computer: Any Computer', 'User: Any User', 'Filename: All Files', and 'Max age: Last Day'.
- Change Policy:** Change policy of computer for a specific computer name or IP address.
- Event Reports:** Summary of activity for the period 10/5/2012 1:39 PM to 10/6/2012 1:39 PM.
 

Report	Files	Computers
<a href="#">New installations</a>	256	31
<a href="#">New unapproved files</a>	1567	31
<a href="#">Blocked files (by bans)</a>	210	14
<a href="#">Blocked files (by unapproved status)</a>	1005	18
- Licensing:** Table showing license types and usage.
 

License Type	Limit	In Use
Visibility	0	0
Control	40	31
- Emergency Lockdown:** A button to 'LOCK DOWN' connected computers not under High Enforcement Level.

The Home Page is a *dashboard*, a configurable page on which you can add and delete *portlets* containing information or controls. See [Chapter 21, “Using and Customizing Dashboards,”](#) for more details on how to use and modify the Home Page and other dashboards. [Table 2](#) below describes the default contents of the Home Page – keep in mind that the Home Page can be modified, so you may see different portlets than the ones described in the table:

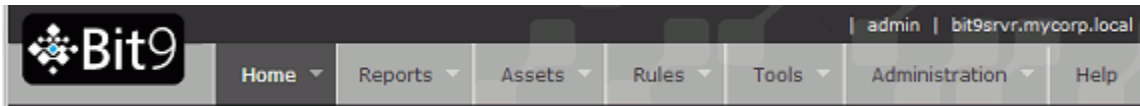
**Table 2:** Home Page Quick Access Portlets

Portlet	Links/Buttons	Description
<b>Alerts</b>	Reset/Reset All Alerts	Shows any triggered Bit9 Alerts that have not been reset, and provides a Reset button for each so you can clear them if you choose. It also provides links from each alert to its Alerts History page for more details about that alert.
<b>Top X</b>	Search/Clear	Shows a table of the top items in various categories – for example, the 10 computers with the most blocked files in the past day. You can specify the number of items to show (default is 10) and the time period over which to look for them (default is 1 day). In the results, clicking on a name (e.g., a computer name) opens a details page for that item. Clicking on a number usually displays the Events page filtered to show events matching your Top X query.
<b>Find Files or Events</b>	Search/Clear	Finds files and events (file blocks, unapproved files, or all events) associated with computers, users or file names you specify. For file name searches, when the "Exact Match" box is checked, only that single file is listed in the results (if found). When the box is not checked, all files containing the string you enter in the box are listed in the results. The Max Age dropdown allows you to determine the time period over which to conduct the search; it defaults to "Last Day".
<b>Event Reports</b>	New installations	Displays a table of all new file installations that have taken place during the past day (24 hours up to the time you display the page) on Windows computers managed by this Bit9 Server. <b>Platform Note:</b> Installations on Mac systems are not included in this <i>New installations</i> table. However, the files that are installed appear in tables that show <i>new files</i> .
	New unapproved files	Displays a table of all new unapproved files that have appeared on computers managed by this Bit9 Server during the past day (24 hours up to the time you display the page).
	Blocked files (by bans)	Displays a table of all banned files that have been blocked on computers managed by this Bit9 Server during the past day (24 hours up to the time you display the page).

Portlet	Links/Buttons	Description
<b>Event Reports (cont.)</b>	Blocked files (by unapproved status)	Displays a table of all new, unapproved files that have been blocked as a result of the Unapproved Executables setting. The report covers the past day (24 hours up to the time you display the page).
<b>Licensing</b>	Manage your licenses	<p>Displays the total number of Bit9 Agent licenses available on your server and the number in use. If some licenses are for Visibility and some for Control, shows the number for each type.</p> <p>Clicking the <b>Manage your licenses</b> link opens the Licensing panel of the System Configuration page, where you can add Bit9 Security Platform licenses, and can configure and activate Bit9 Software Reputation Service (SRS).</p>
<b>Find Computer</b>	Search/Clear	<p>Entering a string that matches all or part of the name or IP address of a computer running a Bit9 Agent displays a list of matching computers. If you click on a computer name in the results, its Computer Details page appears. Computer details include currently Enforcement Levels and connection status. Tabbed views on the page also show details such as last logged in user(s), agent version, and System Details (if available).</p> <p>Computer name searches are not case sensitive.</p>
<b>Change Policy</b>	Change/Clear	Changes the current security policy of a specified computer. Enter the name or IP address of the computer whose policy you want to change in the upper box. Its current policy is shown. Enter the policy you want to change to in the lower box. Once you click <b>Change</b> , the computer moves to the new policy and stays there unless you explicitly move it again.
<b>Emergency Lockdown</b>	Lockdown/Restore	<p><b>Lockdown</b> switches all connected computers managed by this Bit9 Server to High (Block Unapproved) Enforcement Level. Placing computers in High Enforcement Level during high-threat periods helps ensure that no new executable files are permitted to run.</p> <p>When computers are under emergency lockdown, <b>Restore</b> returns them to their pre-lockdown state. If they were in High Enforcement Level prior to the emergency lockdown, they remain in that state.</p> <p><b>Note:</b> Lockdown <i>does not</i> affect systems that are in Local Approval mode.</p> <p>If you do not have any Control licenses, Lockdown is disabled, but Restore is still available in case machines were locked down at a time when you <i>did</i> have full licenses.</p>



## Using the Main Menu



The Bit9 Console main menu at the top of each page allows you to easily navigate to other console pages. The menu is organized in sections according to logical task-groupings, and in most cases shows a submenu of choices when you move the mouse over one of the top-level labels. Clicking on a top-level item opens the page for the first sub choice.

**Table 3:** Bit9 Console Main Menu Choices

Section	Description
Home	<p>By default, the console displays the <i>Home</i> page when you log in. Clicking <b>Home</b> in the menu bar returns to this page from other pages.</p> <p>The Home Page provides quick access to information about files, events, computers, and licenses. It also lets you change the policy of a computer or initiate a network-wide lockdown if needed.</p> <p>The Home Page is a <i>dashboard</i>, which means you can customize it to deliver different information, and can display information in different forms. See <a href="#">Chapter 21, “Using and Customizing Dashboards,”</a> for more details.</p> <p>A dropdown menu on the <i>Home Page</i> lists any other dashboards to which you have access.</p> <p>You can change the page that appears first when you log in to the console. See <a href="#">“Setting Preferences for Console Users”</a> on page 71.</p>
Reports	<p><b>Events</b> are messages resulting from activities monitored by or related to the Bit9 Security Platform. On the Events page, Saved Views provide custom reports for certain types of events, and you can filter any view to create your own report. Events include files blocked, unapproved files executed, and system changes made by console users. For file-related events, you can link directly from an event to the file details.</p> <p><b>Dashboards</b> displays the Dashboard List page. A dashboard displays information about your Bit9 Security Platform installation and the assets it manages through a series of compact “portlets.” You can drill down for more details about files, computers, events and alerts. The Home Page is a special dashboard, and one or more other dashboards may be provided with your Bit9 installation. Users can create and optionally share their own dashboards and portlets.</p> <p><b>Baseline Drift</b> displays a page with two tabs:</p> <ul style="list-style-type: none"> <li>• The <b>Baseline Drift</b> tab shows any available reports that analyze the “drift” from a specified baseline file inventory, allows you to run the reports, and allows you to create and configure new reports.</li> <li>• The <b>Snapshot</b> tab on the Baseline Drift page shows any named file lists, called “Snapshots,” that you have created for use in baseline drift analysis. There are several places in the Bit9 Console from which you can create a Snapshot.</li> </ul> <p><b>External Notifications</b> displays the External Notifications page, which shows a table of notifications from network security devices, such as those from Check Point, FireEye, and Palo Alto Networks. If a file or computer in a notification also appears in Bit9 endpoint data, that data can be correlated with the notification.</p>

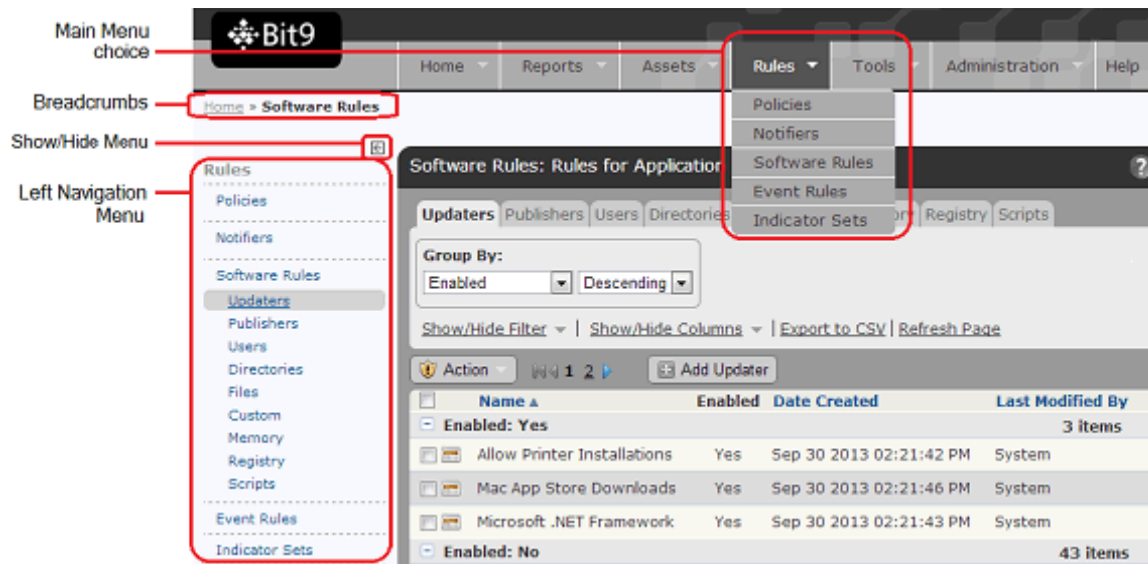
Section	Description
<b>Assets</b>	<p><b>Computers</b> shows a table of computers managed by the Bit9 Security Platform. You can filter the table of computers by various categories. For the computers in the table, you can change the security policy to apply and also put the computer into Local Approval or back into the Enforcement Level determined by its normal policy.</p> <p><b>Files</b> displays the Files page, which shows two tabbed lists of files on your Bit9 Security Platform-managed computers:</p> <ul style="list-style-type: none"> <li>• <b>File Catalog</b> is a list of all <i>unique</i> files that have been discovered by agents reporting to your Bit9 Server.</li> <li>• <b>Files on Computers</b> is a list of all <i>instances</i> of tracked files discovered by agents reporting to your Bit9 Server.</li> </ul> <p>In addition, you can use the Saved Views menu to further specify the files you want to see. Views include Banned Files, New Unapproved Files, Malicious Files, Categorized Files, and Installed Programs.</p> <p><b>Platform Note:</b> The Installed Programs view shows Windows programs only.</p> <p>You can use custom filters on the Files page to locate specific files and ban or approve them (locally or globally) as appropriate.</p> <p><b>Devices</b> displays the Devices page, which shows two tabbed lists of removable devices detected by the Bit9 Security Platform on Windows computers:</p> <ul style="list-style-type: none"> <li>• <b>Device Catalog</b> has two views. One is a list of all unique device <i>models</i> that have been discovered by agents on computers reporting to your Bit9 Server; the other lists all <i>instances</i> (i.e., unique serial numbers) found.</li> <li>• <b>Devices on Computers</b> is a list of all unique <i>attachments</i>, which are defined as pairings of one computer and one device.</li> </ul> <p>You can globally approve or ban any of these devices so that client computers can access files on the approved devices when other devices are restricted or so that files on a specific banned device are never allowed to execute.</p> <p><b>Platform Note:</b> Device discovery and control are currently available on Windows agents only.</p>
<b>Rules</b>	<p><b>Policies</b> shows the table of existing policies (named sets of security rules) and allows you to edit these policies or create new ones. It also provides a link to the Bit9 Agent download page.</p> <p>Each policy automatically generates its own agent installation file when created. The installation file used to install the agent determines the initial policy of a computer, but computers can be moved to another policy or deleted from the policy when retired from service.</p> <p>If you have configured Active Directory integration with the Bit9 Security Platform, a <b>Mappings</b> tab is available on the Policies page. Clicking it opens the Active Directory Policy Mappings page, where you can set rules by which computers running the Bit9 Agent are assigned to Bit9 policies according to one of the Active Directory groups the computer (or its user) belongs to.</p> <p>The Mappings option appears only if the Bit9 Server and an Active Directory server inhabit the same Active Directory Forest, and if you have enabled AD-policy mapping on the System Configuration page. If the Bit9 Server is not in the same forest as the AD server used to identify your users and systems, contact Bit9 Support.</p>

Section	Description
<b>Rules (cont.)</b>	<p><b>Notifiers</b> displays the table of existing blocked file or action notifiers that can be associated with policies and their settings. You can add, delete, and modify notifiers on this page. Notifiers can be configured to appear on an endpoint running the Bit9 Agent when an action is blocked on that endpoint.</p> <p><b>Software Rules</b> displays several categories of Bit9 Security Platform rules for approving or banning files and controlling access to critical computer functions. Each of the tabs shows existing rules, and depending upon the tab, may allow editing, deleting, creating, and/or enabling or disabling of rules:</p> <ul style="list-style-type: none"> <li>• The <b>Updaters</b> tab lists updaters known to your Bit9 Server. Enabling an updater permits end-users to install application updates whenever they become available for download via that application update program. <b>Platform Note:</b> Updaters are platform-specific.</li> <li>• The <b>Publishers</b> tab lists software vendors for which the Bit9 Security Platform can confirm one or more valid digital certificates. Publishers can be approved or banned through this page.</li> <li>• The <b>Users</b> tab lists users or groups trusted with permission to install files on any computer to which they log in with their credentials.</li> <li>• The <b>Directories</b> tab lists authorized approval directories in which all software is approved.</li> <li>• The <b>Files</b> tab lists individual file approvals and bans.</li> <li>• The <b>Custom</b> tab lists custom rules, such as specifying how and where files are allowed to execute or write, whether a file is tracked by the Bit9 Security Platform, and directories in which modifications are not allowed.</li> <li>• The <b>Memory</b> tab lists the Bit9 Security Platform rules controlling retrieval of information about, modification of, and execution (or termination) of specified processes. <b>Platform Note:</b> This feature applies to Windows agents only.</li> <li>• The <b>Registry</b> tab lists the Bit9 Security Platform rules controlling creation, modification, and editing in the Windows Registry. <b>Platform Note:</b> This feature applies to Windows agents only.</li> <li>• The <b>Scripts</b> tab lists rules that define which files are tracked and controlled as scripts in the Bit9 Security Platform.</li> <li>• The <b>Reputation</b> tab appears if Bit9 Software Reputation Service is enabled on the System Configuration/Licensing page. Reputation-based file and publisher approvals can be enabled and disabled on this tab.</li> </ul> <p><b>Event Rules</b> displays the Event Rule table. Event rules specify an action to be performed when an event matches filters you define.</p> <p><b>Indicator Sets</b> displays the Indicator Set table. An Indicator Set is a group of advanced threat detection rules that can be enabled to increase the visibility of suspicious activities.</p>

Section	Description
<b>Tools</b>	<p><b>Meters</b> enable you to monitor the number of executions of files you specify, and the users and computers executing them.</p> <p><b>Alerts</b> provide notifications in the Bit9 Console and via email when certain conditions occur. Alerts can be made policy-specific.</p> <p><b>Find Files</b> enables you to locate all instances of an executable file on computers running the Bit9 Agent on your network. You can make similar searches from the Files page using filters, but Find Files is pre-configured for this purpose.</p> <p><b>Approval Requests</b> displays a list of file approval requests received from users on computers running the Bit9 Agent. Requests are created when a user is blocked from a file action and requests that the file be approved. The Approval Requests page shows request status along with information about the file and the requestor.</p> <p><b>Requested Files</b> displays a page with three tabs, each of which is a table of files. The tabs are:</p> <ul style="list-style-type: none"> <li>• <b>Uploaded Files</b> – This table shows the list and the status of files that a console user requested to be uploaded to the server from an agent computer.</li> <li>• <b>Analyzed Files</b> – This table shows the list and the status of files that a console user or rule requested to be sent to an external device for analysis.</li> <li>• <b>Diagnostic Files</b> – This table shows the list and the status of diagnostic files that a console user requested to be uploaded to the server from an agent computer.</li> </ul> <p><b>Preferences</b> enables each user (including ReadOnly users) to change their password, choose the first page seen upon login, determine the default number of rows on table pages, enable resizable columns, and specify whether the console maintains customizations to a page between visits.</p>
<b>Administration</b>	<p><b>Login Accounts</b> displays the Login Accounts page for creating and managing users of the <i>Bit9 Console</i>. Note that login accounts are not needed for the users of computers running the <i>Bit9 Agent</i>.</p> <p><b>System Configuration</b> provides access to pages for tasks including the server configuration; managing log files; securing communications with agents; configuring backups; downloading software updates; and configuring optional Bit9 Security Platform services, including integration with Active Directory. System configuration features are available only to administrator-level login accounts.</p> <p><b>System Health</b> displays the System Health page, which provides a summary of the state of factors affecting the operation of this Bit9 Server plus more detailed information about specific factors, such as compliance with the operating environment requirements for a server.</p>
<b>Help</b>	<p><b>Using the Bit9 Security Platform</b> displays the user guide for the Bit9 Security Platform in a separate browser window. You also can click Help buttons on other console pages to launch the Help system and display context-sensitive information about the associated page or dialog box.</p>

## Left Navigation Menu and Breadcrumbs

For any console page other than a dashboard, a navigation menu is displayed on the left side of the page. This navigation menu shows the page choices available under the section of the Bit9 Console main menu you currently are in. For example, if you click **Rules** in the top menu and choose **Software Rules** from the menu, the Software Rules page opens with the default tab, Updaters, displayed. To the left of the updaters table, a menu appears showing all of the choices under Rules, and you can click on any of these choices to display its associated page. You can collapse or expand the left navigation by clicking on the boxed arrow button in the upper right of the menu.



When you navigate to a console page, a trail of “breadcrumbs” is shown in the upper left of the page, indicating the path to your current page. In the illustration above, **Home > Software Rules** is the path to the page shown. You can navigate back to a previous location on the path by clicking on it.

## Bit9 Console Tables

Much of the file and computer information you see while using the Bit9 Console appears in tables. Bit9 Console tables list each primary item on the page (for example, each file on a Files page) in its own row with data related to the item. You can control many aspects of the “view” you have of the information in these tables, and if you like a particular view, you can name it and save it. While the emphasis in this section is on *viewing*, Bit9 Console tables also include many of the controls you use to take *action* on files and computers. These actions are described in detail in later chapters.

### Note

This section describes the tables currently used on most Bit9 Console pages. Dashboard pages have different layout and buttons. See [Chapter 21, “Using and Customizing Dashboards”](#) for a description of dashboard elements.

The Files page illustrates many of the typical elements in Bit9 Console tables.

The screenshot shows the Bit9 Console interface for 'Files: All Unique Files'. It features a table with the following columns: First Seen Date, First Seen Name, Product Name, and Global State. The table contains several rows of file entries, including wsdapi.dll and xpsviewer.exe. Above the table are controls for Saved Views, Group By, Max Age, and various filters.

	First Seen Date	First Seen Name	Product Name	Global State
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	wsdapi.dll	Microsoft® Windows® Operating System	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	wsdapi.dll	Microsoft® Windows® Operating System	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	wsdapi.dll	Microsoft® Windows® Operating System	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	wsdapi.dll	Microsoft® Windows® Operating System	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	wsdapi.dll	Microsoft® Windows® Operating System	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	xpsviewer.exe	Microsoft® .NET Framework	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	xpsviewer.exe	Microsoft® Windows® Operating System	Unapproved
<input type="checkbox"/>	Oct 06 2011 09:20:34AM	xamlviewer_v0300.exe	Microsoft® .NET Framework	Unapproved

Tables feature various buttons and menus that enable you to configure results and execute actions. In addition to the Help button that appears on every page, Bit9 Console pages that show tables may include:

- [Table Data Control Links](#)
- [Table Column Resizing](#)
- [Row Action Buttons](#)
- [Checked Row Action Menus](#)
- [“Add” Buttons](#)

## Table Data Control Links

On many Bit9 Console table pages, a row of text links above the table head allows you to take actions on table data. [Table 4](#) shows the possible Table Data Control links (not all appear on all pages).

**Table 4:** Table Data Control Links

Link Text	Action
<b>Show/Hide Filter</b>	Shows or hides the Filters panel, which lets you narrow the number of results returned in the table.
<b>Show/Hide Columns</b>	Shows or hides the Column Settings panel, which lets you specify which columns are displayed and in what order.
<b>Show/Hide Snapshot</b>	Shows or hides the Snapshot panel, which allows you to add selected files to an existing “snapshot” of files or create a new snapshot. Snapshots can be used to measure Baseline Drift. See <a href="#">“Managing Snapshots”</a> on page 539 for more information.
<b>Export to CSV</b>	Saves the information displayed in the current table to a file, using the standard download method for the current browser. Exported data is formatted as a CSV (comma-separated-value) file suitable for opening as a spreadsheet. Time values output to CSV files are recorded in UTC time.
<b>Refresh Page</b>	Refreshes the page view to show the most current data available from the Bit9 Server. This can be useful if you have been on a page for a long period of time or the page contains information known to change frequently.

## Table Column Resizing

One way to control the width of a table is to add or remove columns using the Show/Hide Columns link. You also have the option of resizing table columns. This feature is available when you see vertical borders between columns. You can enable and disable resizable columns on the Preferences page, which you access by choosing **Tools > Preferences** in the console menu.

You change column width by hovering the mouse cursor over a column border, holding down the left mouse button, and moving the mouse. If you make a column narrower than its contents, text is abbreviated with an ellipsis (...) at the end.





## Row Action Buttons

Rows in dynamic tables include information about objects such as client computers, devices, events, reports, or files. Many tables include buttons at the far left of each row that operate on that row.

	First Seen Date	First Seen Name
	Oct 06 2011 08:32:44AM	python.exe
	Oct 06 2011 08:33:53AM	openssl.exe



**Table 5:** Common Row Action Buttons

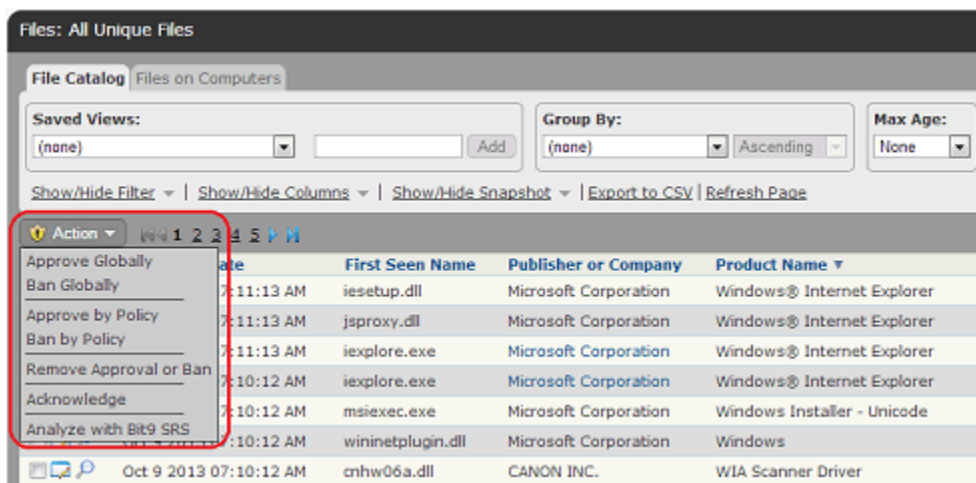
Button	Label	Action
	View Details	Displays details of an item in a row. If the item has editable properties, clicking this button opens its editor.
	Delete	Removes the item in its row from the table and deletes it from the Bit9 database.
	View Report	Displays a report, history, or other information corresponding to the item in a row.
	Find File	Displays the Find Files page and automatically uses the file name or hash of the file in the current row as the search parameter.

**Note**

Different tables include different combinations of row action buttons (not necessarily all of them), as appropriate for the types of information displayed. Some tables have page-specific buttons not shown above.

**Checked Row Action Menus**

On many pages, there is an Action menu with commands that take action on any checked rows in the table on that page. For example, if you are on the File Catalog tab of the Files page and you check the box next to “abc.exe”, the Action menu allows you to globally approve or ban the file, remove an approval or ban if one exists, acknowledge the file, or analyze it in Bit9 Software Reputation Service.





The choices on the Action menu vary according to the page you are on and in some cases the options you have configured.

### Note

Any action you take on checked items affects only the *visible* checked items on the current page. For example, if a Bit9 Console table has three pages and you check items on page 2 and then go back to page 1, the checkmarks are cleared from page 2. If you check some items on page 1 and then choose Approve Globally on the Action menu, for example, only checked items you see on page 1 are approved, even if you previously checked items on other pages.

This also means that when you check the checkbox in the table head, it checks all the items (or all the items that can be acted upon) in the rows on the currently visible page only, not the rows on any other page.

Similarly, when items on a page are grouped, only the visible items in the group can be checked and acted upon. If the group is collapsed (i.e., only the *group name* is showing), none of the items in the group are treated as checked.

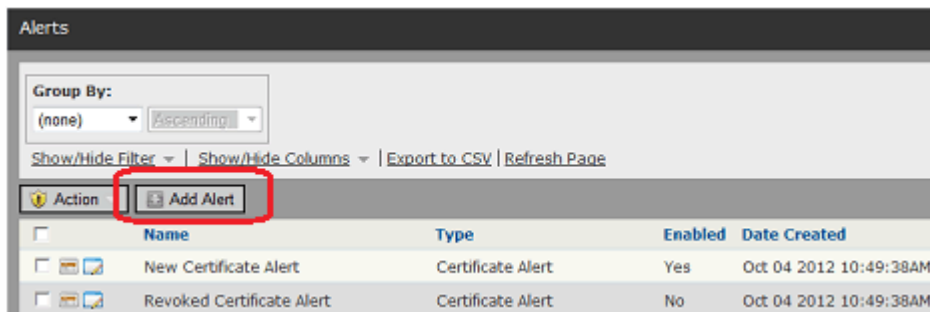
## Row Rank Arrows

On some tables, the ranking of rows affects how the Bit9 Security Platform processes rules. For example, on the Custom Rules page, rule number 1 is processed before rule number 2, etc. These tables show rank numbers for each row, and also can be sorted in rank order.

On table where rank matters, there are arrows in each row (except for special cases) that allow you to move rules so that their rank is higher or lower. In addition, you can drag and drop a row to change its rank in most of these tables.

## “Add” Buttons

On pages where you can create a new instance of something, such as a policy or alert, there will be a button for adding that item. For example, if you wanted to create a new alert, you would go to the Alerts page and click the **Add Alert** button to open a form allowing you to configure the new alert. These Add buttons generally appear in the upper left area of the page.



## Pages, Tabs and Saved Views

Each Bit9 Console page that contains tables provides a specific type of information, such as a table of files, a table of computers, or a table of events. On many pages, you can choose among different “views,” which limit the data on that page to certain parameters, and you can create new views that suit your need. A table page may have one or more of the following features:

- *Tabs* switch you from one major subset of information on the page to another. For example, on the Files page, one tab shows the Files Catalog of all unique files seen by the Bit9 Security Platform and another shows the Files on Computers list of instances of tracked files on every computer.
- *Filters* allow you to limit data in a table to items matching criteria you specify. For example, you can filter a files table to show only those with a particular approval or ban state, or only those with a particular Threat level. Filters can be used with or without saving the views they create.
- *Column controls* allow you to show different information about each item in a table. For example, you can eliminate a column showing the date a file was created but add one that indicates whether anyone has executed the file. As with filters, special column configurations can be incorporated into Saved Views or just used in passing.
- *Saved Views* can filter out unwanted items from the table and also can change the types (columns) of data shown for each item. Bit9 provides pre-configured Saved Views, and you also can create your own. Not all pages have Saved Views.
- *Group By* gives you a menu of choices for different ways to group information in a table. For example, on the Computers page, you can group by Policy, which creates a list of policies, each of which you can click on to show all computers in that policy.
- *Max age* allows you to limit the results shown in a table to those covering a period of time you select on the menu.

You can choose to have the Bit9 Console return each page to its default view when you navigate away from it and come back, or you can have the console “remember” your most recent page view choices and apply them when you next visit the page. See [“Setting Preferences for Console Users”](#) on page 71 for more details.

## Filter Options

Filters let you narrow information displayed in a table so that you can more easily find the data you need. You can select one or more attributes, which correspond to information in table columns, and then enter attribute values on which to search. Operators you can use with the filters vary according to the attribute you select. Depending on the filter you choose, its values can be text, numbers, or dates. For attributes that accept date values, Bit9 Console displays a date box.

**To filter results in a table:**

1. Click **Show/Hide Filters** to open the Filters dialog.

The screenshot shows the 'Files: All Unique Files' interface. At the top, there are tabs for 'File Catalog' and 'Files on Computers'. Below these are three main sections: 'Saved Views' with a dropdown set to '(none)' and an 'Add' button; 'Group By' with a dropdown set to '(none)' and a sub-dropdown set to 'Ascending'; and 'Max Age' with a dropdown set to 'None'. Below these are several utility links: 'Show/Hide Filter', 'Show/Hide Columns', 'Show/Hide Snapshot', 'Export to CSV', and 'Refresh Page'. The 'Filters' section is highlighted, showing an 'Add filter' dropdown menu that is currently empty. At the bottom of the filters section are 'Apply', 'Cancel', and 'Reset' buttons.

2. In the Add Filter menu, select one or more filter attributes you want to use to limit information displayed in the table.

This screenshot shows the same interface as the previous one, but with two filters added. The 'Add filter' dropdown now contains two entries: 'File Type is Application' and 'First Seen Computer is'. The 'File Type' filter has a dropdown set to 'is' and a value dropdown set to 'Application'. The 'First Seen Computer' filter has a dropdown set to 'is' and an empty text input field. The 'Apply' button is highlighted in blue, indicating it is the active action.

3. For each filter attribute, select the appropriate operators and enter values (if required).
4. To filter results by the selected attributes, click the **Apply** button.
5. To return to a display of unfiltered results, click the **Reset** button.

The default operator varies depending upon the attribute you choose, sometimes for performance reasons. For example, “is” is the default operator for File Name in order to limit the amount of data matching the filter.

You usually can add multiple filters of the same type. Two filters of the same type are treated as an either/or operation. For example, if you add a File Name filter for filenames containing “alpha” and another for filenames containing “beta”, the table will show files containing either “alpha” or “beta” in the name.

For the “value” field, that is the data that you want to match, many filters do “auto-completion” as you enter in characters. For example, if you type in “Abc” in a Product Name filter with a “contains” operator, the Bit9 Console displays a menu of all product names that contain “Abc”, and you can pick one from the menu rather than typing in the entire name.

Filters apply only to the level of information currently displayed in a table. For example, if you are displaying a list of file groups (the default) rather than individual files, a filter that looks for First Seen Name containing the text “abc” will only match the names of *installer*

*files* containing that string. It will not match individual files installed by another file. On the other hand, if you click the *Show individual files* box with the same filter in effect, any file containing the filter string installed by the installer will appear in the table.

### Notes

- You can click the Show/Hide Filters button and the Show/Hide Columns button to show both panels at the same time. This combination might provide more insight into how you would like to modify a particular table.
- To save a view that you would like to use regularly, create a new Saved View. See “[Default and Saved Views](#)” on page 66.

## Show/Hide Columns Options

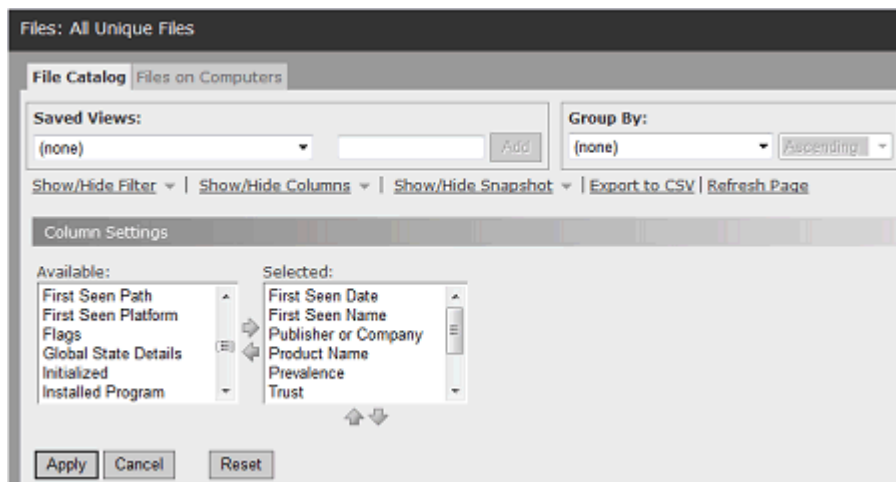
The Show/Hide Columns link opens a Column Settings panel where you specify which columns are displayed and in what order for a particular table:

- Items in the *Selected* column are displayed in the table.
- Items in the *Available* column are not displayed in the table.

Because there is a very large number of possible columns for most pages, not all columns are shown by default, and there are different column defaults for different Bit9 Console pages. You can reset any table to its initial, default columns.

**To show/hide/rearrange information that appears in table columns:**

1. Click **Show/Hide Columns**. The Column Settings panel appears:



2. To hide a currently displayed column:
  - a. Select a column heading in the Selected list.
  - b. Click the left-arrow icon to move the column heading into the Available list.
  - c. To accept changes and update the table display, click the **Apply** button.

3. To display a currently hidden column:
  - a. Select a column heading in the Available list.
  - b. Click the right-arrow icon to move the column heading into the Selected list.
  - c. To accept changes and update the table display, click the **Apply** button.
4. To change column order:
  - a. Select a column heading in the Selected list.
  - b. Click the up arrow or down arrow (below the Selected list) to change the position of the column in the table. The top-to-bottom item order in the list corresponds to a left-to-right orientation of columns in the table. You can only move items that are visible in the table (i.e., column headings that appear in the Selected list).
  - c. To accept changes and update the table display, click the **Apply** button.
5. To restore the table to the default settings for the current view, click the **Reset** button

### Notes

- You can open both the Show/Hide Filters and the Show/Hide Columns dialogs at the same time. The combination of the two might provide more insight into how to best modify a particular table.
- If you use column controls to configure a view that you think you would like to use regularly, you can name it so you can access it again as a Saved View. See [“Default and Saved Views”](#) on page 66.

## Tabs

Tabs switch you from one major grouping of information to another within a page. For example, on the Files page, you can click the File Catalog tab, which (if not modified) shows all of the *unique* files (i.e., not each instance of the same file) discovered on Bit9 Agent-controlled computers on your network. The other tab on that page, Files on Computers, shows all *instances* of all tracked files found on your computers. In some cases, different actions are available on a page when you change tabs.

## Table Length

The bottom of a table page shows the total number of items in the table and the number of pages in the table. It also provides page navigation buttons for moving between pages in the table and a menu for changing the number of rows displayed per page.

The screenshot shows a table with two rows of data. The first row has columns for a file icon, a timestamp 'Oct 06 2011 09:20:34AM', a filename 'sqlrt.dll', a company name 'Macrovision Corporation', and a status 'Approved'. The second row has a similar structure with 'magicdisc.exe' and 'MagictSO, Inc.'. Below the table is a navigation bar with several elements: a set of navigation icons (back, forward, search, etc.), a checkbox labeled 'Show Individual files', a text box showing '9939 items', a text box showing 'Page 1/398', and a dropdown menu showing '25 rows per page'.

If you request an extremely large table, the total number of items in the table (i.e., on all pages, not just the currently displayed page) will show as an approximation, such as *More than 10000 items*, and display the first page of the table. This allows the Bit9 Console to optimize page loading time and also indicates that you might want to request a table with a

more manageable set of data. Consider modifying the view, for example, by changing the *Group By* choice, or sorting by a different column.

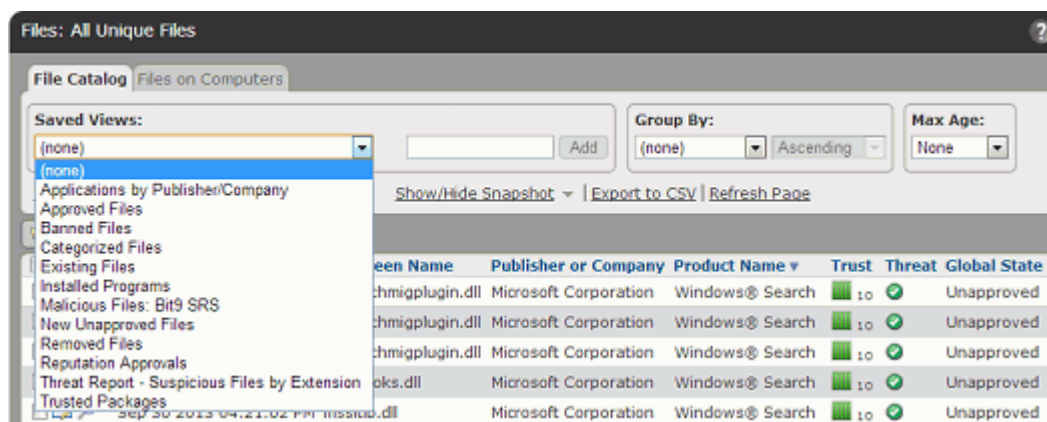
In rare cases, especially with a very large number of Bit9 Agents and/or an underpowered database server, requesting a table with an extremely large amount of data may cause Bit9 Server to time out. Use the techniques mentioned above to reduce the data set.

## Default and Saved Views

Each page and tab has a default view, which is unfiltered and shows data columns assumed to be most commonly of interest. To get exactly the view you want, you might modify several different table parameters. So that you do not have to recreate these modifications every time you view a page, the Bit9 Console allows you to *name* and *save* views on most pages. Once you have named a view, you can get to it again simply by choosing it on the Saved Views menu. When you choose **(none)** on the Saved View menu, you reset the page to the system default view.

ReadOnly accounts cannot create new Saved Views. They can access pre-configured Saved Views and those created by other users.

Most Bit9 Console pages come with pre-configured Saved Views in addition to **(none)**. Although you cannot change pre-configured views, you can use them as templates to create your own new Saved Views.

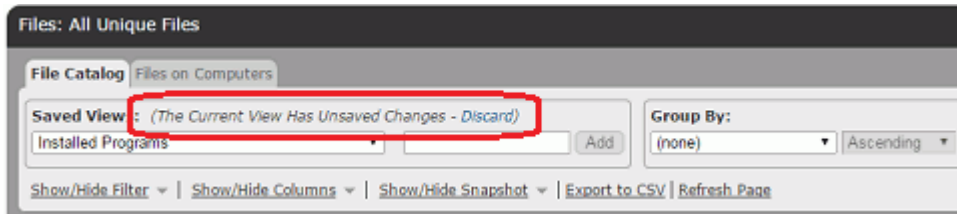


### To display a pre-configured Saved View:

1. Go to the page and tab (if any) you want to view.
2. In the Saved View panel, make a choice from the Saved Views menu. The view is displayed as soon as you release the mouse button.

Depending upon the view you choose, you might see different columns in the table, or only information matching a filter (for example, only files with status “Banned”).

In any view, including *(none)*, you can make your own modifications via the filters and column controls, and also through a variety of other shortcuts on the page that let you set a time period, maximum number of items per page, and grouping. Once you modify a view from its original form, the Saved Views panels shows that you have unsaved changes until you either save the changes or reset the view to another Saved View. Changes to system-provided views must be saved to a different name.



**To create and save a view of a Bit9 Console table:**

1. Go to the page and tab (if any) you want to view.
2. If you want to start with an existing view as your template, choose that view from the Saved Views menu.
3. Use **Show/Hide Columns** to show the columns you want.
4. Use **Show/Hide Filter** to include or exclude items from the table.
5. To view only items newer than a particular date or time, use the Maximum Age menu. (You also can create more complex date/time filters on the Filters menu).
6. To show items listed by a group name rather than the item name, choose a Group from the *Group By* menu and choose the order in which you want them displayed (*Ascending* or *Descending*). For example, to group files by Publisher, choose Publisher. The table initially shows the groups, but if you click on a group name, it expands to show the individual items in that group.
7. On pages that show tables of files, if you want to see individual files installed by an installer rather than the installer file name only, click the *Show individual files* checkbox in the bottom right of the page.
8. If you want more or fewer rows displayed per page, choose a different number from the *rows per page* menu in the bottom right of the page. If you choose *page* in the right menu of this line, the change affects only the page you are on (e.g., only the Computers page). If you choose *all pages* in the right menu of this line, the change affects every page in the console for which you have not specified a length.
9. Once you have exactly the view you want, type a name representing this view into the right box in the Saved View panel and click the **Add** button. Your new view is now saved and available by name from the Saved Views menu.

Note that even if you do not create a Saved View, the Bit9 Console can remember the most recent view (filters and columns choices) for each page, so if you navigate away from the page and come back, you will see your most recent view until you make an alternate view selection. Once you choose a different view, however, any changes to the current view are lost.

If you choose, you can set a user preference that does not remember your most recent view of a page, instead resetting to the Bit9 Console default view when you navigate away from a page. See [“Setting Preferences for Console Users”](#) on page 71 for more details. Also, even if your preference is to remember changes, if you do not want any modifications remembered in a particular visit to the page, you can click on the **Discard** link next to the message about unsaved changes, and this returns the view to its saved format.



## Exporting Bit9 Server Data to Files

The Bit9 Console file export tool downloads data to a file in comma-separated-value format. Downloaded data is presented according to the current column and filter configuration for online display.

If you download the file to a Windows system, it has .CSV extension. On Mac systems using the Safari browser, the downloaded file has the standard CSV format but has a .CSV.XLS extension.

### To download table data to a file:

1. Click **Export to CSV**. The standard download dialog box for your browser appears.
2. Follow the instructions presented in the dialog box to download the file:
  - a. Choose to open the file or save the file to disk.
  - b. If you save the file to disk, select a location and optionally rename the file.

## Details Pages and Object Previews

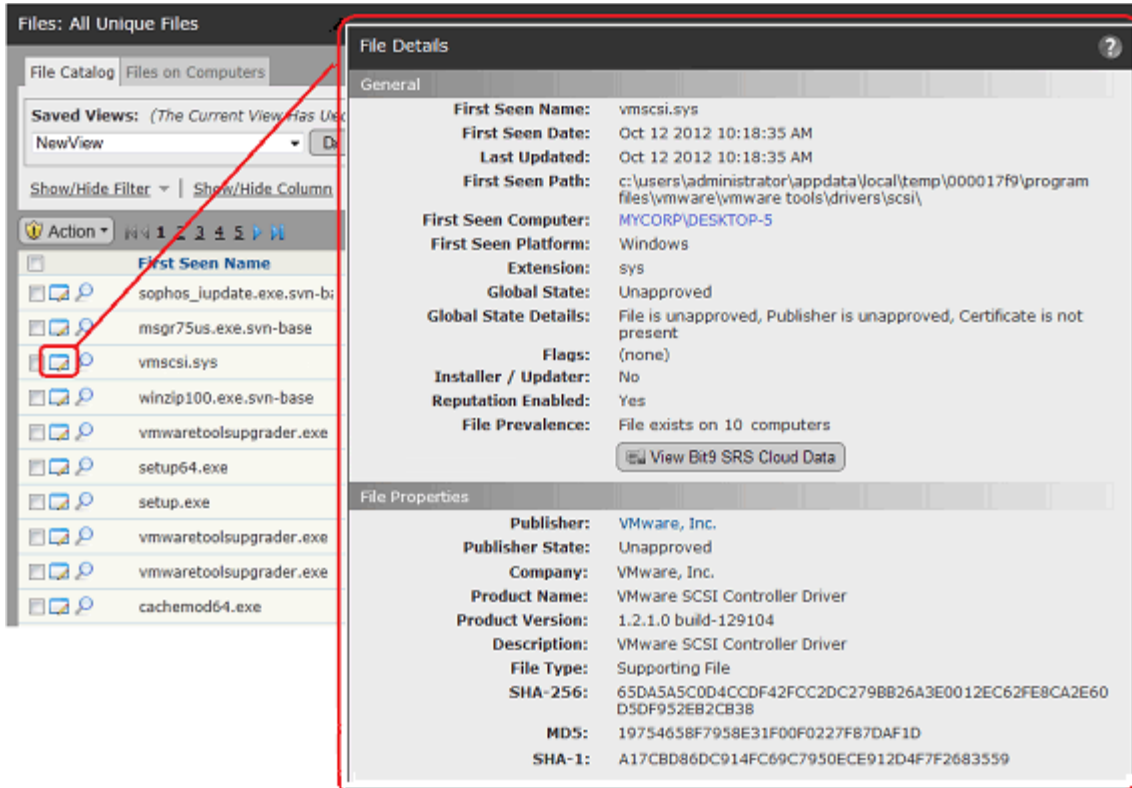
In many Bit9 Console tables, you can get more details about the item in a row by clicking a View Details button or (if it is highlighted in blue) the name of an object in the table.

Details pages include:

- File Details pages
- Computer Details pages
- Publisher Details pages
- Certificate Details pages
- Device Details pages
- External Notification Details pages
- Indicator Set Details pages
- Approval Request Details pages

For example, clicking the details button next to a file name in the Files Catalog brings you to a File Details page, which shows more information about the file. See [Chapter 7, “File and Publisher Information”](#) for more on the file details available in the Bit9 Console.

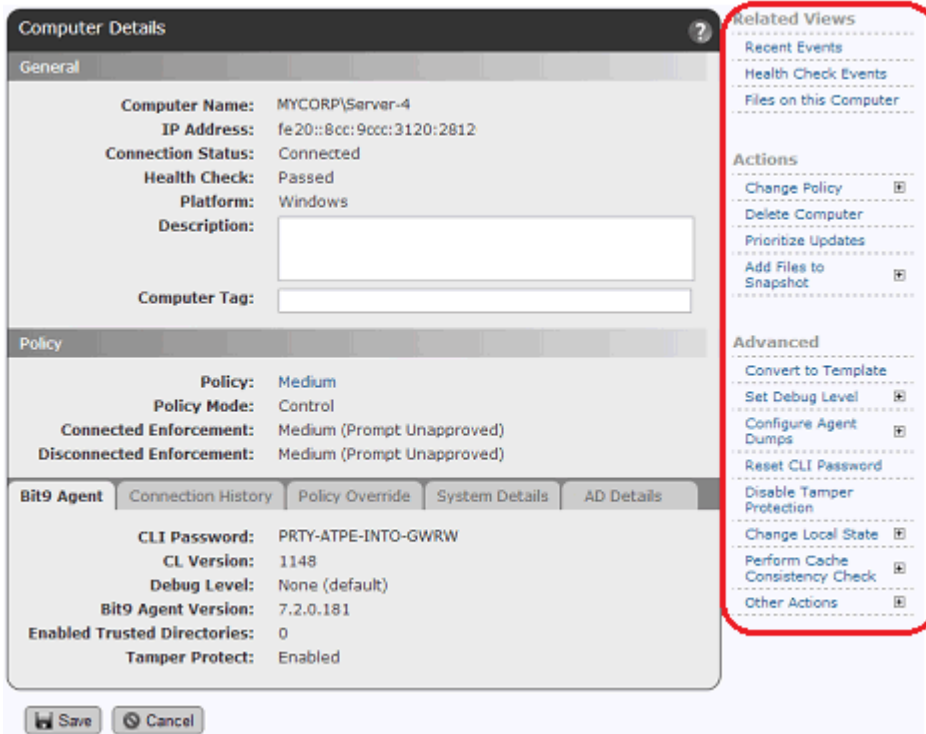




## Menus on Details Pages

Some Bit9 Console pages have menus to the right of the main content. These menus may include one or more of the following sections:

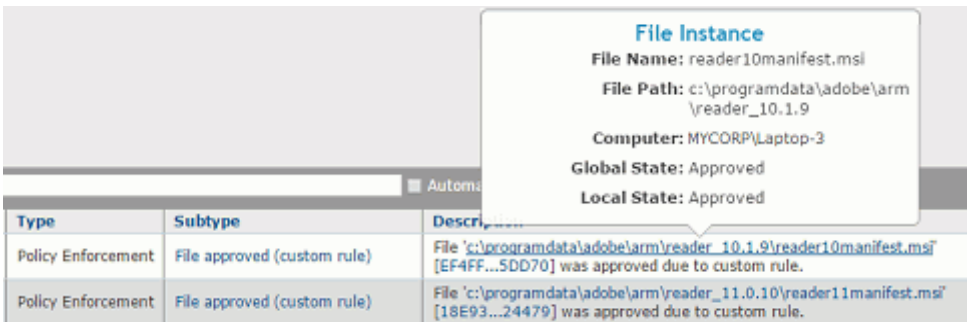
- **Related Views** links send you to pages related to the current page. For example, the Computer Details page includes a link to a table of all tracked files on that computer.
- **Actions** commands take actions related to the content of the page. For example, the File Instance Details page includes commands to ban or approve the current file.
- **Advanced** commands are less common or require consultation with Bit9 support for proper use. For example, the Computer Details page includes a command to reset the password used to manage the current Bit9 Agent.
- **External Pages** links are available if other products are integrated with the server and they are configured for direct links to their information from the Bit9 Console. For example, a Computer Analytics link could take you to the Splunk console.



## Object Previews in Table Data

As the sections above have described, details pages provide a significant amount of information about objects cataloged in the Bit9 database, and one of the ways to get to details pages is to click on highlighted information in a table. In some cases, you might want more than the name of a highlighted object but not all of the information provided by its details page. Object previews provide summary information for many highlighted objects without requiring that you navigate away from the current page.

To see an object preview, move the mouse cursor over a highlighted item without clicking. For example, this is what a File Instance preview looks like when you move the cursor over a file name in the Events page.



The following items in a table have object previews (if they are highlighted):

Following objects will show a preview:

- Files in catalog
- File Instances

- Certificates
- Computers
- Devices
- Publishers
- Policies

## Shortcut Links

On many Bit9 Console pages, there are blue highlighted shortcut links that bring you to pages showing information related to the page you are on. For example, on the Computers page, clicking on a computer name takes you to the Computer Details page for that system while clicking on the policy name takes you to the Edit Policy page.

Action	Date Created	Computer	File Name	Publisher or Company
	Oct 06 2011 09:20:01AM	MYCORP\DESKTOP-7	ora600d.msi	SlikSvn & The SharpSvn Project
	Oct 06 2011 09:20:00AM	MYCORP\DESKTOP-2	60091.msi	Microsoft Corporation
	Oct 06 2011 09:19:59AM	MYCORP\LAPTOP-3	27e95e.msi	VMware, Inc.

On some pages, the link is a quick way to search for information that might otherwise require creation of a complex query on another page. For example, on the Edit Policy page, there is a link that shows you all computers in the policy.

## Setting Preferences for Console Users

The Preferences page allows each Bit9 Console user to change their password, the page they see first when they log in, and whether changes they make to page views are preserved when they navigate away and return to a page. To view the Preferences page, choose **Tools > Preferences** in the main menu.

Changes to the Preferences page apply to the currently logged in Bit9 Console user, and can be specified by any user, including those with ReadOnly access. [Table 6](#) shows the effect of changes specified on this page.

**Table 6:** User Account Preference Page Choices

Panel:Field	Description
<b>Change Password</b>	Allows current user to enter a new console login password for accounts created in the Bit9 Console. Not available for accounts created through Active Directory.
<b>Display Preferences: Remember Page Settings</b>	<p>Allows current user to choose whether page settings are saved (both within and between sessions). This setting applies to all Bit9 Console pages for the current user</p> <p><i>If checked</i>, all page configuration, including filters, columns, and group by settings, is remembered when you navigate away from a page (or logout) and come back to it.</p> <p><i>If not checked</i>, pages return to Bit9 Console defaults when you navigate away from them, and you lose any special layout you applied to them.</p> <p>In the Action menu, <b>Reset Current Settings</b> returns pages to their defaults without requiring you to un-check this box.</p>
<b>Display Preferences: Resizable Table Columns</b>	Allows current user to enable or disable resizable table rows for Bit9 console tables. Enabled by default. See <a href="#">“Table Column Resizing”</a> on page 59 for more information.
<b>Display Preferences: Set Rows per Page</b>	Allows current user to set the standard number of rows per page to be shown on pages that display tables of information. When changed, this re-sets the number of rows on all Bit9 Console table pages. However, each user can customize the rows-per-page for an individual page after the overall preference is set. The default setting is 25.

Panel:Field	Description
<b>Display Preferences: Default Starting Page</b>	Allows current user to choose (from a menu) which Bit9 Console page appears first upon login. Choices are: <ul style="list-style-type: none"> <li>• Home Page</li> <li>• Events</li> <li>• Computers</li> <li>• File Catalog</li> <li>• Policies</li> <li>• Find Files</li> <li>• Approval Requests</li> </ul>
<b>Display Preferences: Unsaved Changes Warning</b>	When checked, displays a warning dialog when this user attempts to navigate away from a page with unsaved changes. The dialog allows the user to leave the page as requested or cancel the navigation to stay on the current page. When unchecked, there is no warning when this user navigates away from a page with unsaved changes.
<b>Save/Cancel buttons</b>	<b>Save</b> saves the user's preference changes. <b>Cancel</b> returns to the previous page the user was on, without saving the changes.

## Using Context-Sensitive Help

The Bit9 Console includes a context-sensitive help system that takes you to information relevant to your current view, but from which you can also navigate to other topics. When you click a Help link or button, a new Help window opens, either as a new tab in your current browser or as a new, popup browser. If it displays as a tab, you can drag the tab off of the current browser to display Help in its own window.

Microsoft Internet Explorer might have popup blocking enabled. In this case, you must allow popup displays from the Bit9 Server if you want to view Help as a popup. Also, you might see a certificate error the first time you open Help – see “[Logging In](#)” on page 48 for information on accepting the certificate.

### To display online documentation from the Bit9 Console:

1. Launch Help either of the following ways:
  - Click **Help** in the main menu to open the table of contents for Bit9 Security Platform Help.
  - Click a Help (question mark) button on any page to see the topic for that page.
2. Once Help is open, to view more topics, click on a book icon or the name next to it in the table of contents to expand the contents tree.
3. To view an alphabetic listing of topics, click the **Index** button.

4. To search key words, from the left Help frame, click the **Search** button and enter the keyword for your search in the Search dialog.

#### Notes

- Unless you close the Help tab or browser, each requested Help topic displays in the same window. However, security measures in Internet Explorer and Firefox prevent an open Help window from coming to the front when you load new topics. Click on the tab or use desktop navigation tools such as **Alt - Tab** to bring Help to the front of your display.
- A navigation anomaly in Chrome causes context-sensitive help pages to display the content immediately *below* the topic heading you requested (for example, the first paragraph in the topic). If you are uncertain that you are in the correct topic, scroll up to the heading.

## Chapter 3

# Managing Console Login Accounts

This chapter explains how to manage access to the Bit9 Console and permissions for specific features.

### Sections

Topic	Page
<a href="#">Login Account Management</a>	76
<a href="#">Account Group and Access Privileges</a>	76
<a href="#">Enabling Console Access via AD Accounts</a>	77
<a href="#">Creating Login Accounts through Bit9 Console</a>	83
<a href="#">Changing Passwords and Other Account Details</a>	85
<a href="#">Deleting Login Accounts</a>	87
<a href="#">Disabling Login Accounts</a>	88
<a href="#">Managing Console Account Groups</a>	89
<a href="#">Creating a New Login Account Group</a>	90
<a href="#">Account Group Permissions</a>	93
<a href="#">Editing a Login Account Group</a>	97
<a href="#">Disabling a Group</a>	97
<a href="#">Deleting a Group</a>	98

## Login Account Management

Each Bit9 Console user must log in to the system with a user name and password. Login Accounts provide system-management professionals and others who use the Bit9 Console the ability to access and manage Bit9 features, and manage or monitor computers running the Bit9 Agent.

There is one built-in login account for the Bit9 Console. The *admin* account provides a way to initially log in to the console, and cannot be deleted. By default, this account has full administrative privileges for everything except File Uploads.

The first thing you should do when you log in as *admin* is change the password (also *admin*). See [“Changing Passwords and Other Account Details”](#) on page 85.

To create additional Bit9 Console accounts, you have two choices:

- You can create accounts in the console. These accounts are managed through the console, and can be deleted by users whose login accounts have the proper privileges.
- You can permit users to log in using Active Directory credentials, if the users belong to certain “mapped” groups. AD-based Bit9 Console logins appear as “External Accounts,” and details of these accounts may be modified only in AD, not in the Bit9 Console. For environments requiring the best security practices, Bit9 recommends using AD-based accounts.

Although you can have a mix of AD-based and console-created login accounts, you should consider your preferred account management strategy before beginning to create new accounts. It is less confusing to generate all of your Bit9 Console accounts in the same way, either as AD-based accounts or as accounts created in the Bit9 Console. Otherwise, although there will not be literal account name duplication, you could have, for example, a console-created account name “fred” and also an AD-based account “fred@somedomain.”

## Account Group and Access Privileges

Users’ privileges are determined by the *login Account Group* they belong to. A user’s account group is set on the Add Login Account page and can be changed on the Edit Login Account page. [Table 7](#) summarizes the default privileges for the four built-in account groups:



**Table 7:** Built-in Login Account Groups and their default capabilities

Login Account Group	Capabilities Summary
<b>Administrator</b>	Complete access to all Bit9 Console features except File Uploads, Extend Connectors with API, and View process command lines. Can add or remove privileges from any user, including itself.
<b>PowerUser</b>	Access to all features except: <ul style="list-style-type: none"> <li>• Can edit own login account but cannot create, edit or delete other users' login accounts, or any account groups</li> <li>• Cannot modify System Configuration pages, access File Upload features, or submit files for analysis.</li> </ul>
<b>ReadOnly</b>	<ul style="list-style-type: none"> <li>• Can view but not create or modify views, rules, or settings in Bit9 Console tables, reports, and details pages.</li> <li>• Can create personal dashboards, but must use existing portlets. These are the only assets they can edit or delete.</li> <li>• Can modify their own password and page view defaults through the Preferences interface.</li> <li>• Cannot access Computer Details page Advanced Options.</li> <li>• Cannot access administrative pages, including Approval Request, Login Account, and System Configuration pages.</li> </ul>
<b>Unauthorized</b>	No access to Bit9 Console.

Built-in account groups cannot be deleted, but the privileges of the Administrator, PowerUser and ReadOnly groups can be edited to enable or disable access to features. In addition, Administrators can create new account groups with custom privileges (including the ability to create accounts and groups). See [“Managing Console Account Groups”](#) on page 89 for instructions on creating account groups and customizing account privileges.

## Enabling Console Access via AD Accounts

If you use Active Directory and the Bit9 Server has been joined to an Active Directory domain, you can use AD accounts to log in to the Bit9 Console. By default, Active Directory accounts are mapped from one of the three specifically-named AD security groups to Bit9 Console accounts groups, as shown in [Table 8](#). The table also shows how other AD groups are mapped.

**Table 8:** Default Mapping of AD Groups Bit9 Console Account Groups

Active Directory Security Group	Bit9 Console Account Group
cn = “Bit9 Administrators”	Administrator
cn = “Bit9 Power Users”	PowerUser
cn = “Bit9 ReadOnly Users”	ReadOnly
cn = <i>(Choose any AD group)</i>	<i>(Matching custom Bit9 account group)</i>
<i>(Unmapped group names)</i>	Unauthorized

When a user logs into the Bit9 Console with an AD-based account, that account is added as a Bit9 Console account. Users attempting to login to the Bit9 Console with a legitimate AD account but who are not members of a mapped group (Administrators, Power Users, Read Only or a custom group) will be added to the Bit9 Console accounts table, but as an Unauthorized account. As such, they will not be able to login to the Bit9 Console.

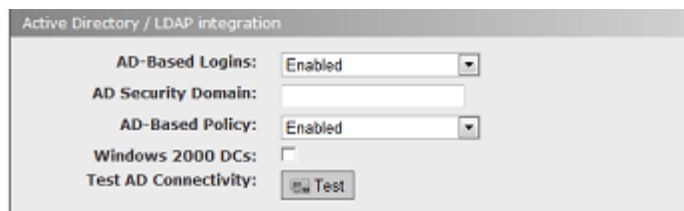
It is best to assign an AD account to only one Bit9-related AD security group. However, since AD groups can be assigned indirectly, it is possible to unintentionally have an AD account assigned to multiple Bit9 security groups. In this case, the Bit9 Console Account Group highest in the ranking list (i.e., with the lowest number) determines that account's Bit9 Server access. See [“Managing Console Account Groups”](#) on page 89 for more details.

### Notes

- If you cannot or choose not to use one of the standard, mapped Active Directory group names, you can map another AD group to any Bit9 Console Account group. See [“Managing Console Account Groups”](#) on page 89 for more details.
- Unless you are using a Windows 2000 domain controller, you can specify a security domain separate from the login domain of your user accounts. This allows you to create Bit9 account groups in the named security domain rather than in the domain for each of your users.

### To enable use of AD logins on the Bit9 Console:

1. For each AD user account that you want to have Bit9 Console access, make sure you have assigned the account to a mapped AD security group.
2. Log in to the Bit9 Console as `admin` or any other administrator account you have created.
3. In the Bit9 Console menu, choose **Administration > System Configuration**. The System Configuration page opens.
4. On the System Configuration page, click on the **General** tab. Initially, the settings on this page are grayed out.



Active Directory / LDAP integration

AD-Based Logins: Enabled

AD Security Domain:

AD-Based Policy: Enabled

Windows 2000 DCs:

Test AD Connectivity: Test

5. Examine the Active Directory/LDAP integration box. If AD-based logins already shows as *Enabled*, you do not have to make any changes and you can skip the remaining steps.
6. If AD-based logins shows a value of *Disabled*, click the **Edit** button at the bottom of the page to make the settings editable.
7. In the dropdown menu for AD-based Logins, choose **Enabled**.

8. If you are using Windows 2000 domain controllers, check the Windows 2000 DCs box. This notifies the Bit9 Server that cross-domain membership features are not available.
9. If you created the AD Security Groups for Bit9 in a domain other than the login domain for the users who will log in to the Bit9 Console, enter that domain in the AD security domain field. (This feature is not available if you are using Windows 2000 domain controllers).
10. Click the **Update** button, and when the Confirmation dialog appears, click **Yes**. You can now use Active Directory login accounts (if from one of the mapped groups) to access the Bit9 Console.

You disable the use of AD-based logins with the same procedure, except that you choose *Disabled* for the AD-based logins setting. If you disable AD-based logins, users will no longer be able to use their AD account names and passwords to access the Bit9 Console.

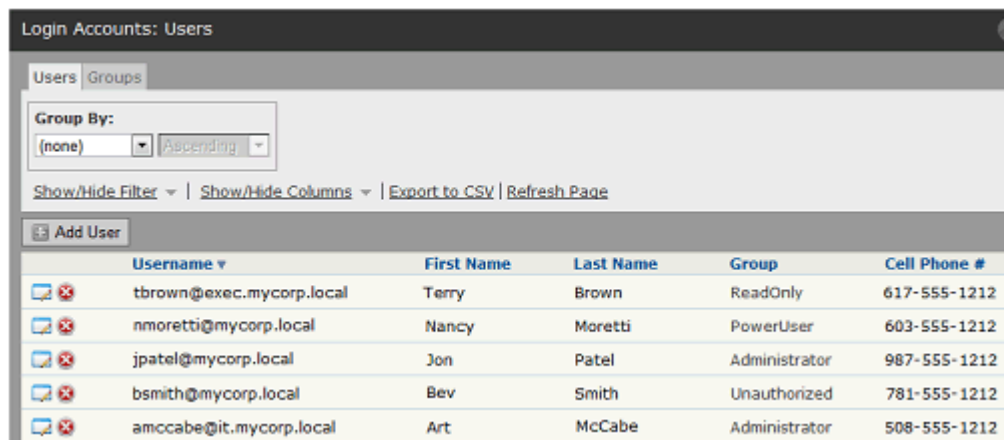
## AD Login Account Format

The format for logging into the Bit9 Console with an Active Directory account name depends upon whether the account name is in the same or a different domain as the Bit9 Server:

- AD accounts in a different domain must use a fully qualified version of their name (i.e., in the format *NTDOMAIN\Username* or *Username@dnsDomain*).
- AD accounts in the same domain as the Bit9 Server can log in either with a fully qualified username or their username only (provided the username is not the same as a login account created directly using the Bit9 Console).

There are several differences in the details for an AD-based account and an account created in the console:

- When a user with an AD-based account logs in to the Bit9 Console, the username on the Login Accounts page and the User Details page includes both the user and the domain name, in the form *user@dnsDomain*.



Username	First Name	Last Name	Group	Cell Phone #
tbrown@exec.mycorp.local	Terry	Brown	ReadOnly	617-555-1212
nmoretti@mycorp.local	Nancy	Moretti	PowerUser	603-555-1212
jpatel@mycorp.local	Jon	Patel	Administrator	987-555-1212
bsmith@mycorp.local	Bev	Smith	Unauthorized	781-555-1212
amccabe@it.mycorp.local	Art	McCabe	Administrator	508-555-1212

- When you click on the View Details button to open the User Details page, the box at the top of the details panel is labeled “External Account” for AD users.

External Account	
User Name:	nmoretbi@mycorp.local
Email Address:	nmoretbi@mycorp.com
Group:	PowerUser

Personal	
Salutation:	Ms.
First Name:	Nancy
Last Name:	Moretti
Title:	Director
Department:	Product Development

Contact	
Home Phone:	
Cell Phone:	603-555-1212
Cell Phone #2:	
Pager:	
Pager #2:	

Comments	
Comments:	
Admin Comments:	

Cancel

- There is no Save button on the Login Account Details page for AD users because their account details can't be edited in the Bit9 Console.

## Adding, Deleting, and Changing AD Login Accounts

The Bit9 Server stores user information for AD accounts that have logged in to the console, but re-validates that information for each login attempt. Any AD account changes that occur while that user is logged in to the console take place only after they log out and log in again. Also, account updates depend upon how frequently the AD domain controllers on the network send out changes. Among the AD account changes that can affect Bit9 Console login accounts are:

- User accounts added to AD become available as Bit9 Console login accounts as long as they meet the security group and forest criteria.
- User accounts eliminated from AD can no longer be used to log in to the Bit9 Console.
- If there is a change in an AD-based user's security group assignment in AD, the user's access level in the Bit9 Console changes when they next login.
- Other Bit9 Console User Details (contact information, etc.) for an AD-based user can be changed in AD and will appear when that user next logs in to the console.

**Notes**

- All of the AD-based login features depend on the Bit9 Server being able to communicate with the AD system and being in the Domain. If for some reason the Bit9 Server cannot communicate with the AD System (due to network setup change, network failure, AD system unavailable, etc.), AD-based Logins will stop working until the condition is corrected.
- AD-based login features also require that AD security groups are defined in each forest that contains users who will access the Bit9 Server; and that users you want to allow access to the Bit9 Server are added to the forest-specific security group.

## Changing AD Group Mapping and Rank

If you have AD mapping enabled, the mapping of AD security groups to Bit9 Console login groups is specified on the Group Details pages for each login group. You can change the AD mapping for any login group, including the built-in groups. See [“Editing a Login Account Group”](#) on page 97 for details.

In general, an AD account should match only one login account group mapping rule. However, in case there are duplicate matches, mapping rules are ranked on the Login Accounts: Groups page. You can change the rank of an AD mapping rule to assure that the rule you want to take precedence is higher than other rules. See [“Changing AD Mapping and Rank of a Group”](#) on page 89 for details.

## Changing AD User Details Displayed in the Bit9 Console

Whether an AD User has a Bit9 Console login account or not, anytime an AD user account appears in a table (other than the Login Accounts page) in the Bit9 Console, additional information can be displayed by clicking on that user name. For example, if you display the Events page, some events include the user associated with the event:

Timestamp	Subtype	Description	User
Oct 20 2011 01:50:50PM	Console user login	User 'admin' logged in from 10.3.4.333	admin
Oct 20 2011 12:52:19PM	Console user login	User 'jpatel@mycorp.local' logged in from 10.2.0.64	jpatel@mycorp.local
Oct 20 2011 12:34:42PM	Console user login	User 'admin' logged in from 10.3.4.325	admin

If the name is an AD username, it should be highlighted in blue, and when you click on it, a User Details window appears (note that this is not the same as the User Details page that appears when you click on a name on the Login Accounts page):

Username:	jpatel@mycorp.local
Name:	Jon Patel
Department:	IT
Company:	Mycorp, Inc.
Office:	Division 2
Address:	9 Main St.
City:	Springfield
State:	MA
Email:	jpatel@mycorp.com
Phone:	413-555-1212
Cell Phone:	508-555-1212

Back

You can change, add, or remove fields from this page by editing the file `UserProps.txt`. This file is located in the “Scripts” subdirectory of the Bit9 Server installation directory. For example, if you accepted the default installation directory, it would be in `C:\Program Files\Bit9\Parity Server\Scripts`.

The file is a two-column, colon-separated list. The Bit9 Console label (for example, “Name”) is on the left, and the AD property displayed for that field is on the right. Be sure to use actual AD object properties for the term on the right of the colon if you edit this file.

Similar customization can be done for AD details displayed about computers in the Bit9 Console.

## Creating Login Accounts through Bit9 Console

The following instructions are for creating login accounts through the Bit9 Console. If you want to use existing Active Directory accounts for Bit9 Console access, see [“Enabling Console Access via AD Accounts”](#) on page 77.

### Note

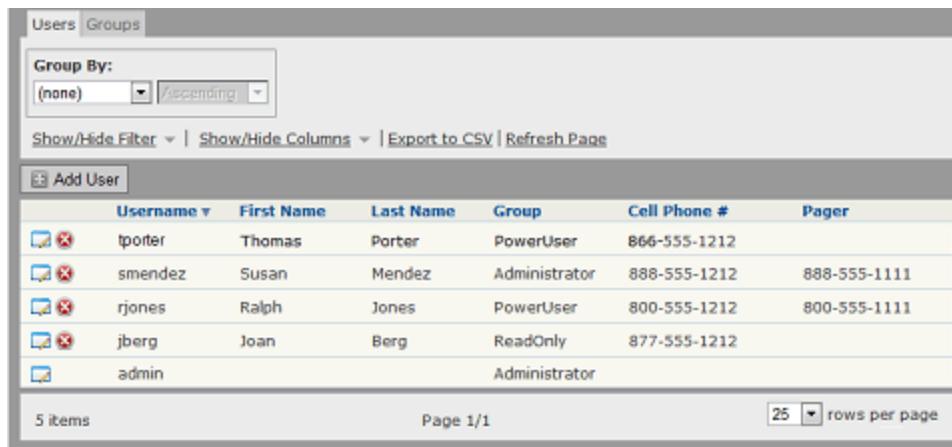
Login Accounts are for access to the Bit9 Console. A login account is not necessary (nor appropriate) for someone whose only Bit9-related role is as a user of a computer that has the Bit9 Agent installed.

Login Account creation privileges depend on account group:

- By default, Administrators can create any level of account.
- By default, PowerUsers and ReadOnly accounts cannot create new accounts.
- Custom account groups have whatever account-creation privileges are shown for the *View login accounts and groups*, *Manage login accounts* and *Manage groups* settings on their Add/Edit Group page.

### To create a console login account:

1. From the console menu, choose **Administration > Login Accounts**. The Login Accounts page appears:



The screenshot shows the Bit9 Console interface for managing login accounts. At the top, there are tabs for 'Users' and 'Groups'. Below the tabs is a 'Group By' dropdown menu set to '(none)' and a 'Ascending' dropdown. There are also links for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', and 'Refresh Page'. A prominent 'Add User' button is visible. Below this is a table with the following data:

Username	First Name	Last Name	Group	Cell Phone #	Pager
tporter	Thomas	Porter	PowerUser	866-555-1212	
smendez	Susan	Mendez	Administrator	888-555-1212	888-555-1111
rjones	Ralph	Jones	PowerUser	800-555-1212	800-555-1111
jberg	Joan	Berg	ReadOnly	877-555-1212	
admin			Administrator		

At the bottom of the table, it indicates '5 items', 'Page 1/1', and a '25 rows per page' dropdown menu.

2. If the Login Accounts: Users page is not displayed, click on the **Users** tab.
3. On the Login Accounts: Users page, click **Add User**.
4. From the Add Login Account page, enter information about the new account in the categories shown in [Table 9](#).
5. After you have filled out the form, click the **Add User** button at the bottom of the page.

**Table 9:** Login Account Details Fields

Field	Description
<b>User Name</b> (required)	<p>Name that the user enters to log in to the Bit9 Console.</p> <p>Enter any combination of letters, numbers, or English-keyboard characters fewer than 32 characters in length. User names are not case sensitive.</p> <p><b>Note:</b> User names should use standard, Latin alphanumeric characters. Symbols and punctuation characters are not allowed. In particular, be aware that user names created in the Bit9 Console cannot contain the “\” or “@” characters. This helps avoid conflicts with AD-based user names using <i>user@domain</i> or <i>domain\user</i> format. If you attempt to create a user account with an illegal character, the Bit9 Console will display a warning dialog.</p>
<b>Password</b> (required)	<p>Password that authenticates this user.</p> <p>Enter any combination of letters, numbers, or English-keyboard characters fewer than 32 characters in length. Passwords are case sensitive. This field changes to New Password when you are editing existing accounts.</p>
<b>Confirm password</b> (required)	<p>Confirm password.</p> <p>Retyping the password ensures that the password is the one you intended to use.</p>
<b>Email address</b>	Email address for the user.
<b>Group</b>	<p>System privileges to be accorded to this user, according to the user’s expected responsibilities. There are four built-in groups. You also can create custom groups with detailed feature-based access control – see <a href="#">“Managing Console Account Groups”</a> on page 89 for details.</p> <p>The built-in account options and their default permissions are:</p> <p><b>Administrator</b> – Full access to all standard Bit9 Console features. Can create, modify, and delete accounts, reports, views, policies, rules, etc., and use any of the System Configuration capabilities. Can modify own permissions.</p> <p><b>PowerUser</b> – Access to most Bit9 Console features; read-only access to System Configuration, Login Account (except own account), and Approval Request sections of console. No access to File Upload or analysis submission features.</p> <p><b>ReadOnly</b> – ReadOnly access to non-administrative features. ReadOnly users cannot change any aspect of the Bit9 Server system configuration, and cannot create, edit, or delete any Bit9 resource. All Administration menu choices are hidden from ReadOnly users.</p> <p><b>Unauthorized</b> – Disables use of an existing account for the associated user. If you want to deny a user access to the system but not delete the account, specify Unauthorized. Privileges cannot be added to an Unauthorized account.</p>
<b>Salutation</b>	Courtesy or professional title of the user (Mr., Ms., Dr., etc.)
<b>First name</b>	First name of the user.
<b>Last name</b>	Last name of the user.



Field	Description
<b>Title</b>	Job title of the user.
<b>Department</b>	Group within the organization to which this user belongs.
<b>Home phone</b>	The user's phone number at home.
<b>Cell phone</b>	Primary mobile phone number.
<b>Cell phone #2</b>	Secondary mobile phone number.
<b>Pager</b>	Primary pager number.
<b>Pager #2</b>	Secondary pager number.
<b>Comments</b>	Further descriptive information that the user can change or enter. This can be any text you would like to display as part of the login account.
<b>Admin comments</b>	Further administrative information about the user. This can be any text you would like to display as part of the login account.
<b>Show API Token</b>	If you check this box, an interface is exposed that allows generation of an API Token for the current user account. It is best to create a special user account for this purpose. See <a href="#">"API Authentication and Access Control"</a> on page 684 for details.

## Changing Passwords and Other Account Details

When you initially log in to the Bit9 Console as *admin*, you should change the default password (also *admin*) to something unique. All users with login accounts, including *admin*, should change their passwords periodically.

For Active Directory-based accounts, password changes and other account information must be changed in Active Directory – they cannot be edited through the Bit9 Console.

For a login account *created* in the Bit9 Console:

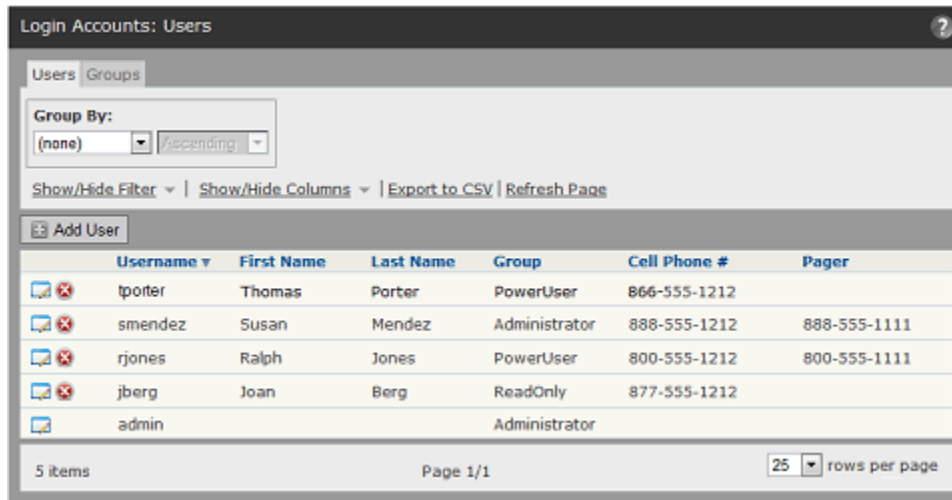
- By default, accounts in the Administrators group may change passwords, contact information, and group for any console-created account. Note that the group for the account *admin* may not be changed.
- By default, accounts in the PowerUsers group may change passwords and contact information for their own account.
- Account-editing privileges in custom groups vary.

### Note

This section describes the Login Accounts administrative interface for changing account details. There is a more limited interface, the Preferences page, on which each account user, including ReadOnly users, can make certain changes to *their own* account only, including changing their password. See ["Setting Preferences for Console Users"](#) on page 71 for details.

**To change a Bit9 Console password and other login account details:**

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears:



2. If the Login Accounts: Users page is not displayed, click on the **Users** tab.
3. On the Login Accounts page, locate the account of the user whose password you are changing, in the Login Accounts: Users table.
4. In the far left column next to the Username, click the View Details icon. The Edit Account Details page opens (see [Table 9, “Login Account Details Fields”](#), for a description of the fields).
5. On the Edit Login Account Details page:
  - a. In the New Password field, enter the new password.
  - b. In the Confirm Password field, enter the password again to confirm it.
  - c. Optionally, change other Login Account Details.
  - d. Click the **Save** button.

**Note**

If the top box on the Login Account Details page is labeled “External Account,” this user accessed the Bit9 Console with an Active Directory account and their details cannot be edited. Accounts created in the console show “Account” as the title for the top box.

6. If you change another user’s password, be sure to inform them of the change.

## Deleting Login Accounts

Login accounts can be removed from the system, for example, when an employee no longer needs access to the Bit9 Console or leaves the company. Bit9 Console users can delete any account type they are allowed to create:

- By default, accounts in the Administrators group can delete any account except their own.
- By default, accounts in the PowerUsers group can delete ReadOnly accounts but not PowerUsers or Administrators.
- Account-deletion privileges of accounts in custom groups vary.

### Note

You cannot delete the default *admin* administration account.

### To delete a login account:

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears:

Username	First Name	Last Name	Group	Cell Phone #	Pager
tporter	Thomas	Porter	PowerUser	866-555-1212	
smendez	Susan	Mendez	Administrator	888-555-1212	888-555-1111
rjones	Ralph	Jones	PowerUser	800-555-1212	800-555-1111
jberg	Joan	Berg	ReadOnly	877-555-1212	
admin			Administrator		

2. If the Login Accounts: Users page is not displayed, click on the **Users** tab.
3. In the Login Accounts: Users table, locate the username.
4. In the far left column next to the user name, click the Delete icon.
5. Respond to the confirmation prompt. To delete the account, click **OK**.

## Disabling Login Accounts

When a user no longer needs access to the Bit9 Console you can restrict access to the console without deleting the login account. You do this by moving the account into the **Unauthorized** group. Users permitted to *create* a particular login account can also disable that account:

- By default, accounts in the Administrators group can disable any account except their own.
- By default, accounts in the PowerUsers group can disable ReadOnly accounts but not Administrators, other PowerUser accounts, or their own account.
- Account-disabling privileges of accounts in custom groups vary.

### Note

Bit9 Console login accounts created through AD mapping cannot be disabled directly. The only way to disable an AD account is to change the mapping rules for their AD security group so that they are mapped to the *Unauthorized* login account group.

### To disable a login account:

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears:

Username	First Name	Last Name	Group	Cell Phone #	Pager
tporter	Thomas	Porter	PowerUser	866-555-1212	
smendez	Susan	Mendez	Administrator	888-555-1212	888-555-1111
rjones	Ralph	Jones	PowerUser	800-555-1212	800-555-1111
jberg	Joan	Berg	ReadOnly	877-555-1212	
admin			Administrator		

2. If the Login Accounts: Users page is not displayed, click on the **Users** tab.
3. In the Login Accounts: Users table, locate the username.
4. Click the View Details icon next to the username whose account you want to disable.
5. From the Group dropdown menu, select **Unauthorized**.
6. Click the **Save** button at the bottom of the page.

## Managing Console Account Groups

The capabilities of a Bit9 Console login account are determined by its account group. A user with permission to manage console account groups can perform the following tasks:

- Create new login account groups with custom privileges.
- Modify the capabilities of the built-in login account groups (except for the built-in Unauthorized group).
- Disable an account group (except for the built-in Administrator group).
- Delete any custom-created account group (but not any built-in group).
- Change the mapping of AD security groups to Bit9 Console login account groups and the order in which mapping rules are evaluated.

You can view the current login account groups on the Login Accounts: Groups page. This page is also the place from which you access other group management features.

### To view the Login Account: Groups page:

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears.
2. If the Login Accounts: Groups page is not displayed, click on the **Groups** tab. The Login Account: Groups page appears.

Name	Status	AD Rank	AD Mapping	Date Modified	User Count
Administrator	Enabled	1	Bit9 Administrators	Oct 25 2011 04:08:33PM	3
PowerUser	Enabled	3	Bit9 Power Users	Oct 14 2011 08:49:49AM	6
ReadOnly	Enabled	4	Bit9 Readonly Users	Oct 14 2011 08:49:49AM	20
Unauthorized	Enabled	5		Oct 26 2011 10:30:22AM	62

## Changing AD Mapping and Rank of a Group

When AD integration is enabled, the Groups tab shows the AD mapping and AD Rank of Bit9 Console login account groups. Rank determines the order in which AD mapping rules are evaluated, which is significant if an AD security group would match more than one mapping rule. You can change rank using the arrow keys on the Login Accounts: Groups page.

Note that “Unauthorized” is permanently assigned the lowest rank because it is the default group for AD security groups that don’t match the mapping for any other Bit9 Console login account group.

## Creating a New Login Account Group

Although the built-in account groups provide options for user access level, the Bit9 Console allows users with sufficient permission to create and modify custom login account groups. You might want to have a special user group whose level of access falls between two of the built-in options. Creating a special login account group can not only prevent unauthorized access to critical features but also might make it easier for users with limited roles to learn those roles without having to see features they will not use.

For example, you might want to allow members of a helpdesk team to view all Bit9 Console information available through the console but only to be able to change policy for a computer, put a computer into local approval, or access debugging features. You can create an account group with these characteristics.

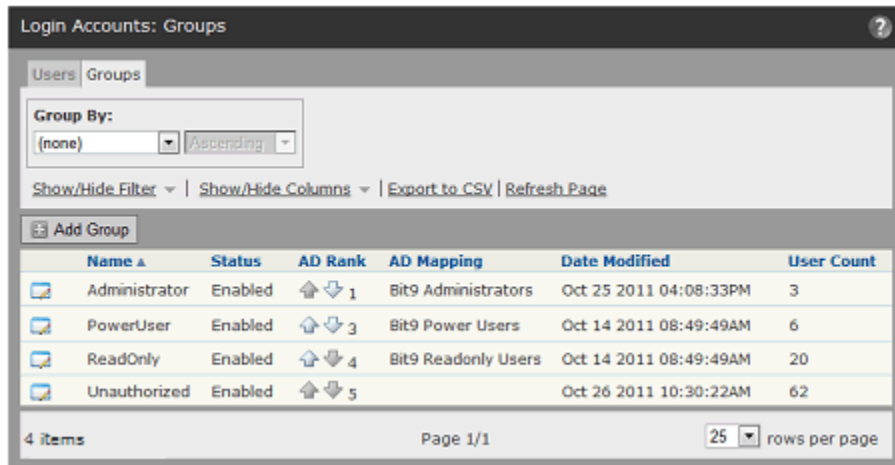
[Table 10](#) shows the information used to define a login account group.

**Table 10:** Login Account Group Parameters

Field	Description
<b>Name</b> (required)	Name that will appear in the Login Accounts: Groups list and will be used when assigning a group to a login account.  Enter any combination of letters, numbers, or English-keyboard characters fewer than 32 characters in length. Group names are not case sensitive.  <b>Note:</b> User names created in Bit9 Console cannot contain the “\” or “@” characters. This helps avoid conflicts with AD-based user names using <i>user@domain</i> or <i>domain\user</i> format.
<b>Description</b>	Optional descriptive information about this group, such as who should be in it and perhaps a high-level summary of its permissions.
<b>AD Mapping Name</b>	If AD-based login mapping is enabled, the AD security group that you would like mapped to this Bit9 Console login group.
<b>Status</b>	Determines whether this group is Enabled or Disabled. Note that disabling a group disables the accounts within it, and prevents AD-mapping from matching this group.
<b>Permissions</b>	A table of checkboxes that determine what members of this group are allowed to do in the Bit9 Console. See <a href="#">Table 11, “Permissions Settings for Login Account Groups,”</a> on page 93 for a complete description.

**To create a new Bit9 Console login account group:**

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears.
2. Click on the **Groups** tab.



3. On the Login Accounts: Groups page, click the **Add Group**. The Add Group page appears.

Asset	Permission	Enabled
Computers	View computers	<input type="checkbox"/>
Computers	Temporary assign computers	<input type="checkbox"/>
Computers	Manage computers	<input type="checkbox"/>
Computers	Change advanced options	<input type="checkbox"/>
Files	View files	<input type="checkbox"/>
Files	Manage files	<input type="checkbox"/>
Files	Change local state	<input type="checkbox"/>

4. Enter a name for the new group, and optionally, a description to make clear the purpose, intended members, or any other information about the group.
5. Assuming you want this group to be available immediately for login accounts, leave the Status radio button set to Enabled.

- If you have AD account mapping enabled and want to automatically map members of an AD security group to this Bit9 Console group, put the name of the AD security group in the AD Mapping Name box.

Asset	Permission	Enabled
Computers	View computers	<input checked="" type="checkbox"/>
Computers	Temporary assign computers	<input type="checkbox"/>
Computers	Manage computers	<input checked="" type="checkbox"/>
Computers	Change advanced options	<input checked="" type="checkbox"/>

- Check the box next to each permission you want to enable for this group, and uncheck any permissions you do not want this group to have. See [Table 11](#) for a complete list of permissions.
 

**Note:** If you are giving this group permission to perform most Bit9 Console activities, it might be more efficient to click the Enabled box in the table header, which checks all boxes, and then remove the few permissions you *don't* want to provide.
- When you have finished configuring this group, click **Save** at the bottom of the page. The new group appears in the Login Accounts: Groups table. Notice that it includes a delete button since, unlike a built-in group, a user-created group can be deleted.

Name	Status	AD Rank	AD Mapping	Date Modified	User Count
Help Desk	Enabled	1	IT Helpdesk	Oct 20 2011 02:57:57PM	12
Administrator	Enabled	2	Bit9 Administrators	Oct 25 2011 04:08:33PM	3
PowerUser	Enabled	3	Bit9 Power Users	Oct 14 2011 08:49:49AM	6
ReadOnly	Enabled	4	Bit9 Readonly Users	Oct 14 2011 08:49:49AM	20
Unauthorized	Enabled	5		Oct 26 2011 10:30:22AM	62

- If you have AD mapping enabled, a new group is first in the mapping rank – that is, any AD account matching the mapping name for this new account will be assigned to it, even if the AD account matches other console accounts lower in ranking. If you want the new account to rank lower, use the arrow keys in the AD Rank column to move the new group down in rank, or to move another group up.
- If you are not using AD mapping to assign console login accounts, manually assign any accounts you want to this new group.



## Account Group Permissions

On the Add/Edit Group page for a group, the Permissions table shows the capabilities that can be enabled or disabled for members of the group – items that are checked are enabled and items that are not checked are disabled. You can customize permissions to achieve exactly the level of access you want for a group. The only group for which you cannot change permissions is the Unauthorized group.

For the most part, permissions can be divided into two categories: viewing permissions that allow you to see a particular page or dialog in the Bit9 Console, and management permissions that allow you to create, edit, and delete managed assets, rules, and console users. Some permissions depend on others – you cannot manage something if you can't see it. If you disable *View system configuration*, for example, *Manage system configuration* is automatically disabled as well.

The checkboxes for permissions that depend upon other permissions are gray (instead of white) when they are not enabled. In addition, permissions that depend upon other permissions are indented to make the relationship between them clearer.

### Notes

- Carefully consider any permissions changes you make, especially to the built-in Administrator group. In particular, avoid removing permissions to view and manage user accounts and groups since this will make it impossible to restore access to these features without the use of special recovery commands.
- The Bit9 Console user interface, including pages, menus and links, is documented based on users having the full administrative permissions. Any permissions that are turned off will remove related user interface elements. Consider making users with restricted permissions aware of this possibility so that they are not confused by the absence of features described in Bit9 Security Platform help.

**Table 11:** Permissions Settings for Login Account Groups

Asset	Permission Name	Description
Computers	View computers	Ability to view computer pages
Computers	Temporary assign computers	Ability to generate temporary Enforcement Level override codes. Requires View computers permission.
Computers	Manage computers	Ability to manually assign computers to policies and change Enforcement Level. Ability to manage template computers.
Computers	Change advanced options	Ability to change advanced computer options such as collection of computer diagnostics and re-synchronizing.

Asset	Permission Name	Description
Files	View files	Ability to view files pages.
Files	Manage files	Ability to approve, ban, and acknowledge files. Ability to mark files as installers. Note that this does not include the ability to directly change local file state.
Files	Change local state	Ability to change local state of files on computers.
Devices	View devices	Ability to view device pages.
Devices	Manage device rules	Ability to manage device rules.
Policies	View policies	Ability to view Policies page.
Policies	Manage policies	Ability to manage policies (changing mode, Enforcement Level, etc.)
Policies	Manage policy mappings	Ability to manage automatic policy mapping rules.
Software Rules	View software rules pages	Ability to view Software Rules pages. Also allows viewing of Event Rules page for servers licensed for the Bit9 Connector for Network Security Devices.
Software Rules	Manage event rules	Ability to manage event rules. Requires separate license for the Bit9 Connector for Network Security Devices. <b>Note:</b> Some event rules require other permissions for the actions they specify, such as file upload and analysis and file approval.
Software Rules	Manage trusted directories	Ability to manage trusted directories.
Software Rules	Manage publisher rules	Ability to manage trusted publishers.
Software Rules	Manage trusted users	Ability to manage trusted users.
Software Rules	Manage custom/registry/memory rules	Ability to manage custom, registry and memory rules.
Software Rules	Manage updaters	Ability to enable, disable, and add software updaters.
Software Rules	Manage custom scripts	Ability to manage custom definitions of what the Bit9 Server treats as scripts
Software Rules	Manage indicator sets	Ability to enable, disable, and create exceptions for indicator sets used in advanced detection

Asset	Permission Name	Description
Reports	View events	Ability to view event pages.
Reports	View process command lines	Ability to view process command lines for events. <b>Important:</b> Command lines may include confidential information such as passwords. This permission is not enabled by default, even for administrator accounts, and should be limited to those who require it.
Reports	Manage shared dashboards	Ability to manage shared dashboards.
Reports	View drift reports and snapshots	Ability to view snapshots, drift reports and drift report results.
Reports	Manage drift reports	Ability to manage baseline drift reports.
Reports	Manage snapshots	Ability to manage snapshots used in drift reports.
Reports	Manage saved views	Ability to manage saved views on all pages.
Tools	View alerts	Ability to view alert pages.
Tools	Manage alerts	Ability to manage alerts.
Tools	View meters	Ability to view meters and meter results.
Tools	Manage meters	Ability to manage meters.
Tools	View approval requests	Ability to view user-generated requests for approval of blocked files and justifications of files approved by users.
Tools	Manage approval requests	Ability to manage user-generated requests for approval of blocked files and justifications of files approved by users.
Tools	View file uploads	Ability to view uploaded files on the Requested Files page.
Tools	Manage uploads of inventoried files	Ability to initiate manual file uploads from agent computers, and to create event rules that upload files. This permission applies only to files considered "interesting" (i.e., executables and scripts) by Bit9. Requires separate license for File Uploads.

Asset	Permission Name	Description
Tools	Manage uploads of files by pathname	Ability to initiate manual file uploads from agent computers, and to create event rules that upload files. This permission applies to <i>all</i> files on agent computers, even if not in the Bit9 inventory. Requires separate license for File Uploads.
Tools	Access uploaded files	Ability to download files that are uploaded on the server. Requires separate license for File Uploads.
Tools	Submit files for analysis	Ability to submit files for analysis by network security devices, either manually or through creation of an event rule. Requires separate license for the Bit9 Connector for Network Security Devices, unless implemented through the API.
Notifiers	View notifiers	Ability to view the details of blocked file notifiers.
Notifiers	Manage notifiers	Ability to edit blocked file notifiers or create new ones.
Analytics	View external analytics reports	Ability to view and use links from Bit9 Console to external analytics reports (if external analytics is enabled and configured)
Administration	View system configuration	Ability to view system configuration pages.
Administration	Manage system configuration	Ability to manage system configuration.
Administration	View login accounts and groups	Ability to view login accounts and groups.
Administration	Manage login accounts	Ability to manage login accounts.
Administration	Manage groups	Ability to manage user groups.
Administration	View System Health Indicators	Ability to view the system health page and system health alerts.
Administration	Extend connectors through API	Ability to register and unregister connectors with the Bit9 Server through the Bit9 APIs so that they can send notifications and (if part of their feature set) analyze files.

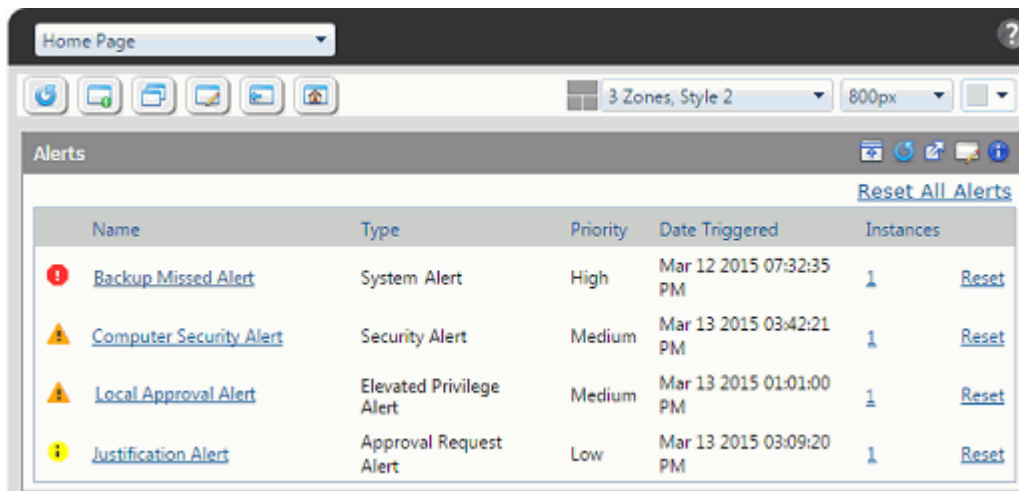
## Editing a Login Account Group

You can edit a Bit9 Console login account group in the following ways:





- You can add and subtract permissions at the feature level for the built-in Administrator, PowerUser, and ReadOnly console account groups, and for any custom group shown on the Login Accounts: Groups tab.
- If you have AD mapping enabled, you can change the AD security group that is mapped to a console login group.
- You can enable an account group, activating the ability of accounts in the group to access the Bit9 Console, or you can disable the group, cutting its members off from console access.
- You can edit the optional Description for a group.

### To change permissions or other properties of a Bit9 Console login account group:

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears.
2. Click on the **Groups** tab.
3. On the Login Accounts: Groups page, click the View Details button for the account group whose privileges you want to change. The Edit Group page appears.



The screenshot shows the Alerts page in the Bit9 Console. At the top, there is a 'Home Page' dropdown menu and a toolbar with icons for home, refresh, and other actions. Below the toolbar, there is a '3 Zones, Style 2' dropdown and a '800px' resolution indicator. The main content area is titled 'Alerts' and contains a table with the following columns: Name, Type, Priority, Date Triggered, and Instances. There is also a 'Reset All Alerts' link at the top right of the table.

Name	Type	Priority	Date Triggered	Instances
 <a href="#">Backup Missed Alert</a>	System Alert	High	Mar 12 2015 07:32:35 PM	1 <a href="#">Reset</a>
 <a href="#">Computer Security Alert</a>	Security Alert	Medium	Mar 13 2015 03:42:21 PM	1 <a href="#">Reset</a>
 <a href="#">Local Approval Alert</a>	Elevated Privilege Alert	Medium	Mar 13 2015 01:01:00 PM	1 <a href="#">Reset</a>
 <a href="#">Justification Alert</a>	Approval Request Alert	Low	Mar 13 2015 03:09:20 PM	1 <a href="#">Reset</a>

4. On the Edit Group page, review the current permissions for each capability shown. Capabilities with checkmarks in the right column are enabled; capabilities with an empty checkbox are disabled. Click the checkbox for any capabilities whose status you want to change.
5. Make any other group properties changes you want, such as the AD Mapping Name or Description and click the **Save** button at the bottom of the page to save your changes.

## Disabling a Group

Any group except Administrator can be disabled. If a group is disabled, all of the logins associated with it become invalid (except for AD-based logins that match another console login group). To disable an *account*, see “[Disabling Login Accounts](#)” on page 88.

## Deleting a Group

Custom login account groups may be deleted *if* there are no accounts associated with them. Built-in account groups may not be deleted.

### To delete a Bit9 Console login account group:

1. From the console menu bar, choose **Administration > Login Accounts**. The Login Accounts page appears.
2. Click on the **Groups** tab.
3. Click the Delete (x) button next to the group you want to delete and confirm the deletion.

## Chapter 4

# Managing Computers

This chapter explains how to manage client computers using the Bit9 Console. It assumes that you already have set up policies, as described in [Chapter 5, “Creating and Configuring Policies.”](#)

Computer configuration tasks include choosing the method for assigning each computer to a security policy, downloading Bit9 Agent, and installing the agent on client computers. This chapter also describes setting up a computer to provide a snapshot of files as a point of reference as new files populate your network.

If you will be managing virtual machines, see [Chapter 6, “Managing Virtual Machines,”](#) in addition to this chapter.

### Sections

Topic	Page
<a href="#">Computer Configuration Overview</a>	100
<a href="#">Assigning Computers to a Policy</a>	102
<a href="#">Downloading Agent Installers</a>	112
<a href="#">Installing Bit9 Agents</a>	113
<a href="#">Upgrading Bit9 Agents</a>	119
<a href="#">Uninstalling Bit9 Agents</a>	127
<a href="#">Viewing the Table of Computers</a>	128
<a href="#">Viewing Complete Details for One Computer</a>	132
<a href="#">Moving Computers to Another Policy</a>	143
<a href="#">Moving a Computer to Local Approval Mode</a>	146
<a href="#">Adding Computers</a>	146
<a href="#">Deleting Computers</a>	146

# Computer Configuration Overview

Client computer systems become visible to the Bit9 Server when you install and run the Bit9 Agent on them. When you download and install the agent, an initialization process begins, delivering information about the computer and its files to the Bit9 Server.

## Pre-Installation Activities

You make some key computer configuration decisions prior to installation of the agent:

- **Policy creation** determines the groups of security settings available to computers. See [Chapter 5, “Creating and Configuring Policies,”](#) if you have not yet created policies.
- **CLI Management** configuration options allow you to designate a user or group, or a password usable by anyone, to perform certain agent management activities in conjunction with Bit9 Technical Support. *Especially if you have systems that will be permanently offline*, it is best to choose one of these options *before* creating policies and distributing agent installation packages. See [“Advanced Configuration Options”](#) on page 627 for more details.
- **(Optional) Review the expired certificate validation setting**, especially if you will be running offline systems. If you intend to allow file approval by certificates that have expired, make this choice before you download and install the agents on permanently offline systems. Otherwise, they will not be able to use expired certificates. See [“Approval with Expired Certificates”](#) on page 244 for more details.
- **Initial Policy assignment** to a computer can be determined by Active Directory data, as described in [“Assigning Policy by Active Directory Mapping”](#) on page 103; or by the agent installer used, as described in [“Downloading Agent Installers”](#) on page 112.
- **(Optional) Preparing a reference computer for a “snapshot” of files** can give you a baseline for the files in your environment. Ideally, this is a clean computer onto which you install only the applications that you would like to run on some or all of your systems. Once the computer is prepared, you can install the Bit9 Agent and, after initialization is complete, use the Snapshot process as described in [Chapter 19, “Monitoring Change: Baseline Drift Reports.”](#)

## Installation and Initialization

For each security policy you create, an *agent installer* is created for each supported platform (i.e., Windows, Mac, Linux). Each agent installer includes the policy assigned to the computer and the Bit9 Server address. If you do not use AD-based policy assignment, you choose the agent installer for each computer based on the computer’s platform and the policy you want to control that computer. Installers are described in the sections [“Downloading Agent Installers”](#) on page 112 and [“Installing Bit9 Agents”](#) on page 113.

As soon as the Bit9 Agent software is installed, file initialization begins. The agent takes an inventory of all executable files on the client computer’s fixed drives (but not removable drives) and creates a hash of each file. When a computer first connects to the server, its agent sends each hash to the Bit9 Server to update the server’s file inventory. Files on a computer at initialization receive a *local* state of Approved unless they already have been identified and globally banned or banned by policy on the Bit9 Server. During initialization, the computer is protected by whatever security policy is assigned to it, and file activities are allowed or blocked according to that policy.



**Note**

Virtual machines cloned from template computers can be configured to include or not include their initial (cloned) files in their inventory. See [“Configuring Clone Inventory”](#) on page 185 for more details.

Unless pre-banned or pre-approved by a Bit9 rule, files that the Bit9 Server has never seen before will get the *global* state of Unapproved and be added to the catalog. If a file was first seen on this agent *after* initialization, it will also get the *local* state of Unapproved on the agent. For more information on file state, see [“File State, Whitelisting and Blacklisting”](#) on page 41.

## Post-Installation Activities

After you have installed the Bit9 Agent on a computer and initialization has completed, there are many ways for you to monitor and manage your computers, including:

- **Viewing Computer Details** – Bit9 Server keeps details about each computer running a Bit9 Agent, including the computer’s IP Address, whether it is currently connected to the server, the policy, mode and Enforcement Level it is assigned, computer model and system details, and its connection history. See [“Viewing the Table of Computers”](#) on page 128.
- **Viewing Computer-related Events** – You can monitor events related to a specific computer. See [“Event Reports”](#) on page 482.
- **Changing Policy** – You can change the security policy assigned to a computer if necessary. See [“Moving Computers to Another Policy”](#) on page 143 and [“Restoring Computers from the Default Policy”](#) on page 144.
- **Creating Clones** – If you plan to use a computer as the template for cloning other computers, see [Chapter 6, “Managing Virtual Machines.”](#)
- **Locally Approving Files** – You can temporarily put a computer into Local Approval mode so that files with a global state of Unapproved on the Bit9 Server can be installed locally and locally approved on this computer. See [“Moving a Computer to Local Approval Mode”](#) on page 146.
- **Viewing Details of Connected Devices** – You can track and manage fixed and removable storage devices on agent-managed Windows computers. See [“Viewing Devices on Computers”](#) on page 330 for more details.
- **(Optional) Saving a Snapshot** – Once agent installation and initialization is complete, you can instruct the Bit9 Server to save a named snapshot of all files (by hash) on this computer currently inventoried by Bit9. This provides a reference point for analyzing changes in file inventory for that computer, other computers, or your whole network. See [“Creating and Modifying Snapshots”](#) on page 539 for more details.
- **Deleting Computers** – If a computer is going to be removed from your network or from Bit9 Security Platform control, you can uninstall the agent and remove the computer from the table of computers on the server. This requires a specific series of actions detailed in [“Deleting Computers”](#) on page 146.

## Access to Computer Management Features

Access to computer management features depends upon the Login Account Group Permissions for the user attempting access:

- Administrator and PowerUser accounts with default permissions have full access to these features.
- ReadOnly users with default permissions can view the details of computers running Bit9 Agents but cannot add, delete, or change their configuration.
- The access level of users in custom login account groups depends on the group's permissions in the Computers asset rows on the Add/Edit Group page. Note that some features described here require additional permissions.

See [“Account Group Permissions”](#) on page 93 for full details on viewing and changing login account group permissions.

In addition to standard computer management features, some or all users can be allowed to access agent management commands that can be used in special situations, usually in consultation with Bit9 Technical Support. See [“Configuring Agent Management Privileges”](#) on page 615 for more details.

## Assigning Computers to a Policy

Every computer running a Bit9 Agent is assigned a security policy. There are three standard ways a computer can be assigned its policy:

- **By Agent installer** – Every policy you create generates a policy-specific Bit9 Agent installer for each Bit9-supported platform, so when you install the agent on a computer, it is assigned a policy. When the agent contacts the Bit9 Server after agent installation, the computer is added to table of computers in the console. If you have not set up AD-based policy assignment, the agent remains in the policy embedded in its installer unless you manually reassign it.  
You do not have to (nor should you) reinstall Bit9 Agent to make a policy change for a computer. You normally only need to install the agent once per computer.
- **Automatically, by Active Directory (AD) group mapping** – You can set up the Bit9 Server to run a script that assigns new and, if configured, existing computers to security policies according to the AD group information of the computer (or the user logged in on it). A computer's initial policy is defined by the agent installer. If that initial policy is configured to allow automatic policy assignment, this AD-based policy assignment takes precedence. Policy assignment by AD mapping is described later in this section.
- **Manually** – You can move any computer to a policy other than the one assigned by the installer or the AD-mapping facility. This might be useful if you discover that a particular computer used the wrong installer, or that its security policy should differ from other computers in the AD group used to map its policy. Manual assignment also might be used for a temporary situation that requires more or less restriction for a computer or its user. If you change a computer's policy manually, you can later restore it to its original policy (or to automatic assignment). Manual policy assignment is described in [“Moving Computers to Another Policy”](#) on page 143.

You can move computers from manual to automatic policy assignment and vice-versa.

**Note**

In certain cases, policy may be changed for reasons other than those listed above. For example:

- If a computer belongs to a policy and you delete that policy while the computer is offline, the computer moves to the Default policy group. See [“Restoring Computers from the Default Policy”](#) on page 144 for more detail.
- There is an optional Event Rule action that can move computers to a different policy when a specified event occurs. Enabling this feature requires the assistance of Bit9 Technical Support. See [“Creating and Editing Event Rules”](#) on page 428 for more details.

If you are *not* using AD-based policy assignment, you can skip the next section and go directly to [“Downloading Agent Installers”](#) on page 112 for instructions on choosing a policy-specific installer.

## Assigning Policy by Active Directory Mapping

You can create rules that map each computer to a certain policy based on its Active Directory (AD) data. AD-based policy assignment happens when an agent first contacts the Bit9 Server, and is checked again each time the server and agent re-establish contact or the logged-in user on the agent computer changes (see [“Computer Registration and AD Mapping”](#) on page 111 for more on when mapping can change).

### AD Policy Mapping Summary

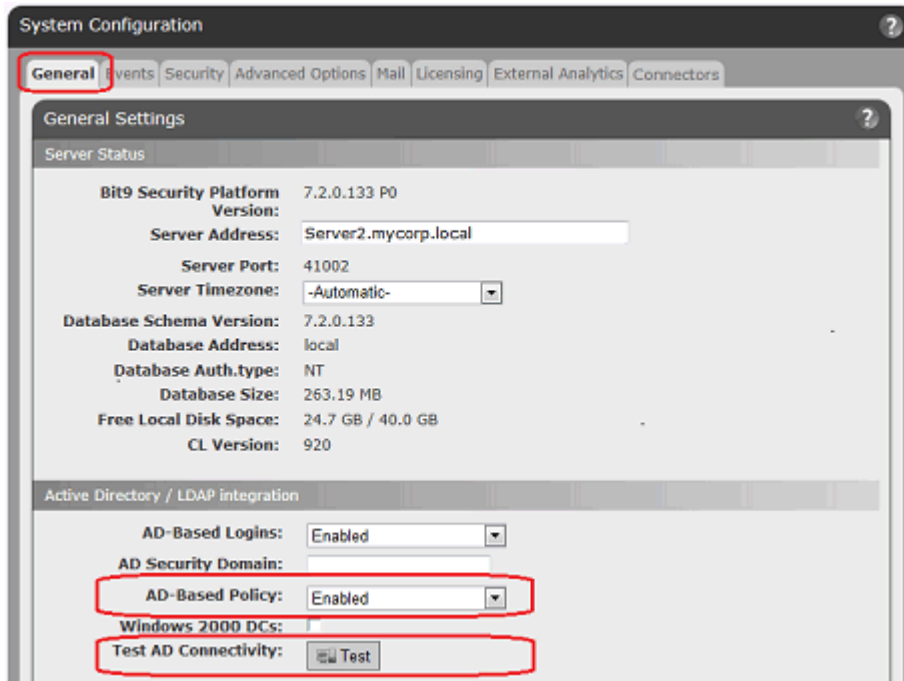
To make use of AD-based policy assignment, you must:

- **Install the Bit9 Server in an AD Domain** – Install the Bit9 Server on a computer that is a member of an Active Directory domain. By default, the Bit9 Server must be in the same AD forest as the computers and users you want to map. If you require cross-forest integration, contact your Bit9 Support representative.
- **Enable the AD Mapping Interface** – You enable the AD-based policy mapping interface in the Active Directory / LDAP integration panel on the General tab of the System Configuration page.
- **Create AD-mappable Target Policies** – Create the security policies to which you want computers assigned by AD Mapping, and make sure these policies allow automatic policy assignment.
- **Create Mappings** – On the Mappings tab of the Policies page, create AD Policy Mapping rules that use AD data to assign computers to different security policies
- **Install or Move Agents to AD-mappable Policies** – For new agent installations, make sure the policy for the agent installation packages allows automatic policy assignment. For mapping to be successful, both the current policy of an agent and the policy to which will be mapped must have automatic policy assignment enabled. For existing agents, if necessary, you can change a policy from manual to automatic after installation or move the agent to an AD-mappable policy.

**Platform Note:** The Bit9 Server will do AD-mapping for any computer you have configured through your Active Directory server, including those on non-Windows platforms.

**To enable the AD Mapping interface:**

1. In the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. If the General Settings view is not already displayed, click the **General** tab. The second panel on the General tab is Active Directory/LDAP integration.



3. In the Active Directory/LDAP panel, click the **Test** button next to Test AD connectivity. If you see a *Success* message, continue to the next step. If you see an *Error* message, your Bit9 Server is unable to access AD. AD Mapping will not work until you correct the problem.
4. If AD connectivity succeeds, click the **Edit** button at the bottom of the window.
5. In the *AD-based Policy* dropdown menu, choose **Enabled**.
6. To submit the changes, click the **Update** button and choose **Yes** on the confirmation dialog.

## Creating AD Mapping Rules

After the AD-based Policy interface is enabled, a new tab, “Mappings,” will be visible when you view the Policies page. Clicking on this tab opens the Active Directory Policy Mappings page. This is where you create rules to map computers with specified AD data to certain policies.

Before you begin setting up mapping rules, be sure you have created all of the policies to which you want computers mapped.

You can create mapping rules that test for matching AD data including organizational units, domains, security groups, computer names, and user names. Keep the following in mind when creating mapping rules:

- Although you can choose to match AD Security Group data for either users or computers, Bit9 recommends computer-based rules. With multiple users on a computer, sometimes simultaneously logged on, AD Mapping rules based on users could lead to unexpected results.
- The Bit9 Security Platform does not support policy mapping for AD object names that contain double quotes. Object names with double quotes cannot be handled properly by the directory object browser you use to create a mapping rule.
- In general, you should create as few rules as possible and use them to test for groups rather than individual objects.

Table 12 shows the rule parameters you provide for a mapping rule.

**Table 12:** AD Mapping Rule Parameters

Parameter	Description
<b>Computer Object to Test</b>	The object that will be tested to see whether it matches the rule. The choices are Computer, User, and User or Computer.
<b>Relationship</b>	The relationship being evaluated between the Directory Object specified in the rule and the AD data from the computer being assigned a policy. The choices are: <ul style="list-style-type: none"> <li>• is member of group</li> <li>• is in OU or domain</li> <li>• is</li> <li>• is not in any domain</li> </ul>
<b>Directory Object</b>	The object in AD that the data from the tested object must match. Clicking the right end of this field opens an AD browser from which you can search for an object from your AD environment.  The choices for the Directory object field change depending upon which Relationship you choose. If you choose "is not in any domain," no Directory object is necessary.
<b>Policy to Apply</b>	The policy to apply to a computer if its tested object matches the rule. The dropdown menu shows all available policies.  <b>Note:</b> For policies created before implementation of Active Directory policy mapping, "Automatic policy assignment" is off by default. If you implement AD policy mapping and set up new mapping rules that apply to a pre-existing policy, you will need to change the setting on the policy itself for automatic mapping to take place. See " <a href="#">Creating Policies</a> " on page 151 for more on automatic assignment choices.

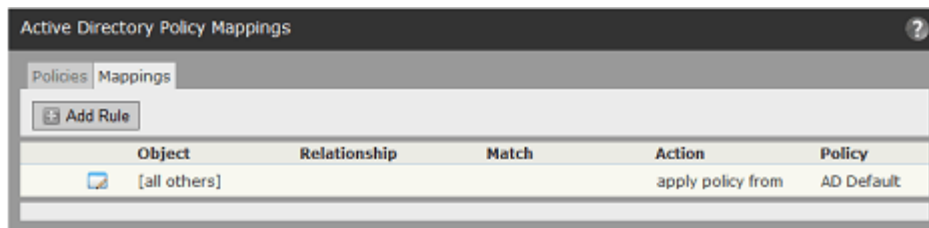
The result of providing these parameters is a rule that can be read like a sentence. The following is how you might set up one rule.

Parameter	Example (value in bold)
<b>Computer Object to Test</b>	If a <b>Computer</b> ...
<b>Relationship</b>	... <b>is in OU or domain</b> ...
<b>Directory Object</b>	...matching <b>OU = Marketing,DC=hq,DC=xyzcorp,DC=local</b> ...
<b>Policy to Apply</b>	... assign that computer to the <b>Standard Protection</b> policy.

The procedure below shows how to configure a mapping rule. Although entry of most of the parameters are reasonably straightforward, pay particular attention to the Directory Object field, which requires use of a special AD browser.

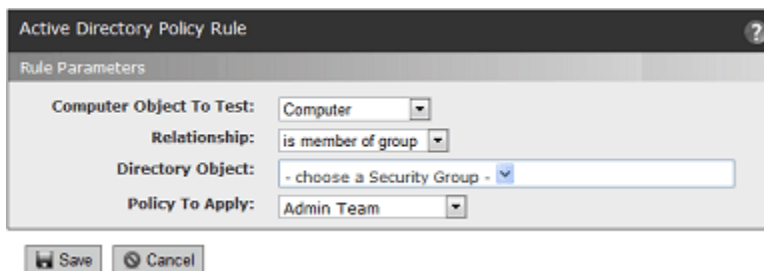
**To create an AD policy mapping rule:**

1. In the console menu, choose **Rules > Policies**. The Policies page opens showing a list of all available policies.
2. Click the **Mappings** tab. The Active Directory Policy Mappings page appears with the Policy Mappings table, initially showing only the default rule.



**Note:** If no Mapping tab appears, the AD mapping interface has not been enabled. Go to the General tab of the System Administration page and enable the feature.

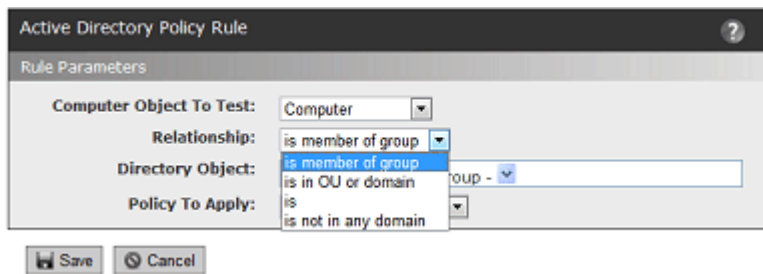
3. On the Active Directory Policy Mappings page, click **Add Rule**. This displays the Active Directory Policy Rule panel in which you enter the rule parameters.



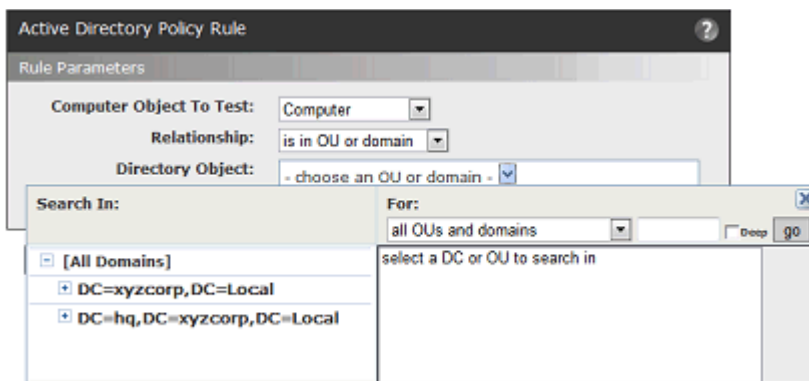
4. Choose the Computer Object to Test (Computer, User, or Computer and User) from the dropdown menu. In most cases, **Computer** is the best choice.
5. Choose the Relationship between the data of the object tested and the Directory Object specified in the rule. The choice for this field changes the choices available in the other fields.

In this field, you can specify that objects must be in a OU or domain, a security group, in no domain, or that they exactly match the directory object you choose (the “is”

choice on the Relationship menu). Generally it is best to choose a relationship that maps multiple computers to a policy rather than one that singles out an individual computer or user.

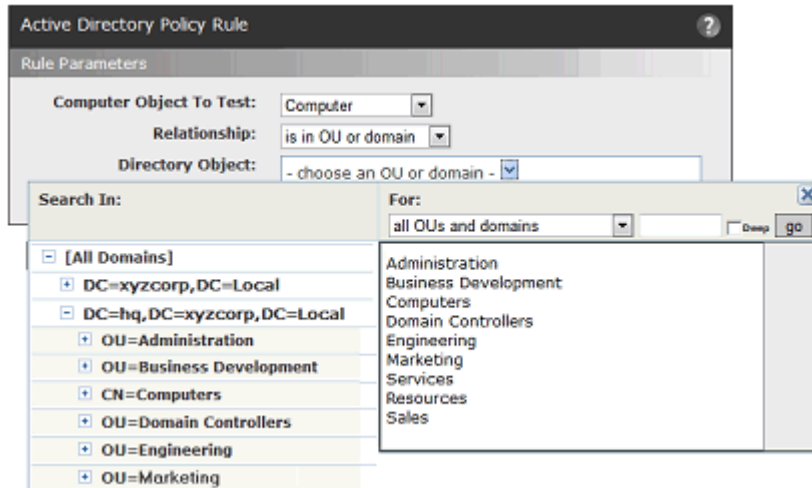


6. Choose the Directory Object that the data from the tested computer must match.
  - a. Click in the *Directory Object* field to open the AD browser. The browser opens immediately below the Directory object field. The left panel is labeled “Search in,” and shows a tree of your AD domains

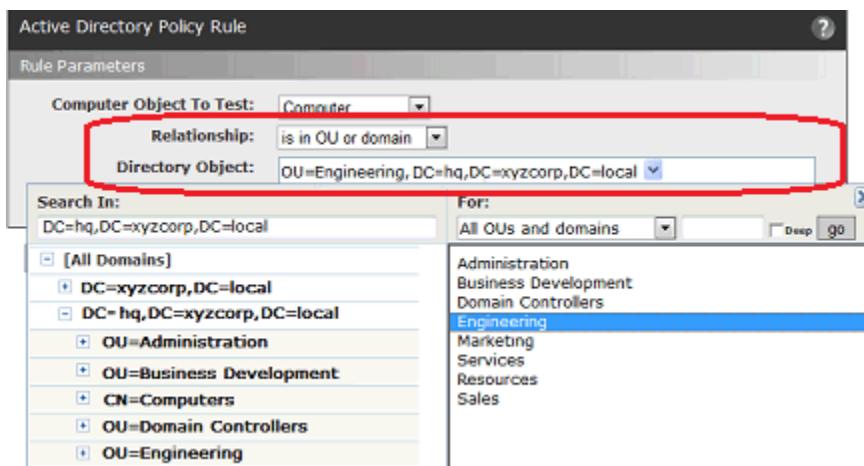


- b. To expand the AD tree in the left panel, click on the plus button, next to the node you want to expand. To collapse the view on the left, click the minus button next to the node you want to collapse.
    - c. Click on the object in the left pane that defines the scope of your search. For example, if you have two domains, you might click on one of them, such as “DC=hq,DC=xyzcorp,DC=Local” in the example above.





- d. If you see the object in the right panel that you want to use for this rule, double-click on it. The object, including full information about its location in the AD object tree, appears in the *Directory Object* field of the Rule Parameters panel and the browser will close.

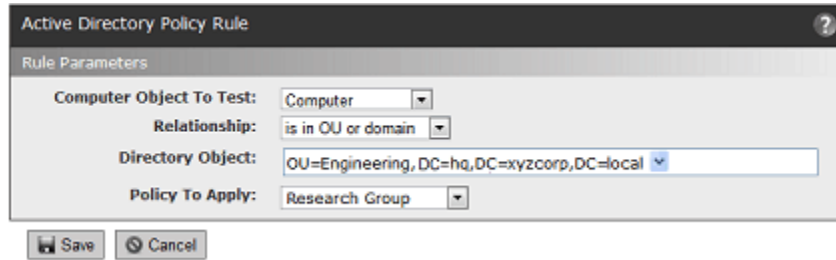


- e. If your actions did not automatically close the browser, click the 'X' button in the top right corner to close it.

**Note:** There are additional options for using the directory object browser. See [“AD Object Browser Options”](#) on page 109 for more information.

7. From the *Policy to Apply* dropdown menu, choose the policy you want assigned to computers that meet the requirements of this rule. Only existing policies appear on the dropdown – if the policy for this rule has not been created yet, cancel the creation of this rule and go to the Policies page to create the new policy.





8. When you have entered all of the parameters for the rule, click **Save**. A newly created rule goes to the bottom of the table of AD rules, just above the default rule, and all rules above it take precedence. In the example, the rule instructs the Bit9 Server to assign any computer belonging to the Engineering OU in the domain *hq.xyzcorp.local* to the Research Group policy.

	Object	Relationship	Match	Action	Policy
↓	if Computer	is	IT-1	apply policy from	Master Privileges
↑	if Computer	is in OU	Domain Controllers	apply policy from	Controllers
↑	if Computer	is in OU	Engineering	apply policy from	Research Group
↑	if Computer	is in OU	Administration	apply policy from	Administration
↑	if Computer	is not in any domain		apply policy from	Highest Security
	[all others]			apply policy from	AD Default

Rolling the mouse cursor over the **i** button next to an object in the Match column provides a description of the object.

9. If necessary, use the up- and down-arrow buttons on the left side of each rule (or the drag-and-drop method) to change the order in which the rules are evaluated against a computer. Remember that the [all others] rule always is the last one in the table.
10. Repeat this procedure beginning with step 3 for any other rules you need to create.

## Mapping Rule Ranking

AD Mapping rules are scanned in top-to-bottom order on the Mappings page, and only the first match on the list is applied. You can rearrange the order of rules if you find that you would prefer a different policy assignment outcome than you are seeing.

There is a default AD Mapping rule that cannot be deleted, nor can it be moved from the bottom of the Policy Mappings rule table. It maps “[all others]”, that is, all computers that have not matched any of the other rules in the table, to the policy you choose. Because it remains at the bottom of the table, it assures that any automatically mapped computer is assigned to some policy. It is initially mapped to the Default Policy, but you can change this. Creation of an “AD Default Policy” is recommended so that computers not matching other rules have a policy that best reflects a default security level with settings you want.

## AD Object Browser Options

This section describes the AD Object browser, which you use to select a Directory object when defining an AD Mapping rule, in more detail.

The left panel of the AD Object browser is where you determine the scope of your search. It displays an AD tree with “[All Domains]” at the top of the tree and then shows the contents of the tree in standard browser format, with +/- buttons at each node that contains other objects so that you can collapse or expand the tree at that point.

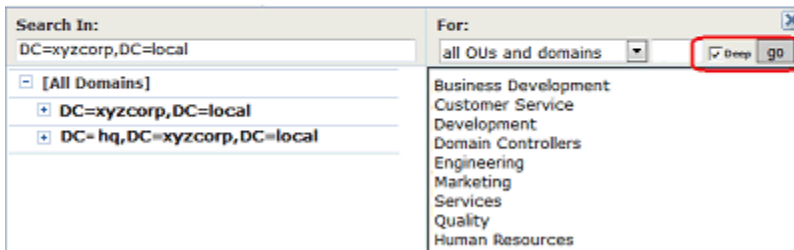
The right panel has a description of what you are searching for, based on the “Relationship” value you entered in the Active Directory Policy Rule parameters. When you click on a node in the tree on the left, all objects immediately under that node matching the “Relationship” (e.g., “OUs and domains”) appear in the right panel. You click on an object in the right panel to select it and enter it in the Rule Parameters panel.

### Object Search Depth

In the upper right area of the browser, there is a checkbox labeled “Deep”. When you check the Deep box and click **Go**, this results in a multi-level search that examines not just the immediate contents of the selected node but the contents of any nodes inside it, regardless of how many layers deep they are. Notice the greater number of results in the right panel of case B in the illustration below.



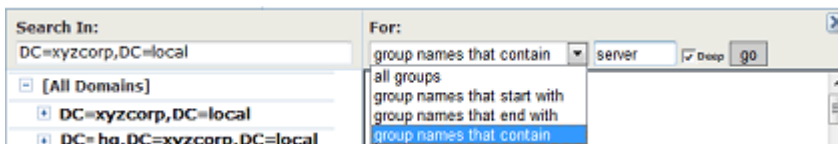
A. Results of a standard search in an AD domain



B. Results of a Deep search in the same domain

### Object String Match

Another option in the AD Object browser is searching by string match. If you enter a string of characters in the box immediately to the left of the “Deep” checkbox, you can search for AD objects in the selected node that start with, end with, or contain the string. You make the choice of how to use the string via the dropdown menu to the left of the text box. For example, if you entered “eng” in the text box and then searched for “group names that contain” the string, you would match both “Engineering” and “System Engineering” groups if they existed in the node selected on the left.



## Computer Registration and AD Mapping

Certain events trigger registration of a the agent on a computer with its Bit9 Server. When this occurs, the following conditions may affect AD policy mapping:

- When the Bit9 Agent is first installed, the computer will register with the server for the first time, with the users that are logged on at the time. If no users have logged on since the last time this computer was started, the Bit9 Server shows an empty user list for that agent computer.
- When an agent computer is restarted, if the Bit9 Agent reconnects to the server before any user logs in, the user list for that registration will be empty.
- All agent computers (whether or not they use automatic policy assignment) re-register whenever their list of user sessions changes.  
**Platform Note:** Because of the way Windows handles sessions, a user's session on a Windows computer does not necessarily end upon logout. It persists until it is replaced by a different user's session.)
- Agent computers are disconnected by the server whenever the server restarts and re-registered when they reconnect to the server.
- The server disconnects a computer (forcing re-registration) whenever the agent computer's policy assignment is changed manually, or if it is changed from manual to automatic.

## Clearing the Server AD Cache

The AD information that is used to map agent computers to policies is cached on the Bit9 Server and updated every four hours. It is also updated whenever a Bit9 Security Platform rule change occurs that is related to AD mapping.

If you make a change to this AD information on your AD server – for example, changing the group a computer or user is in, or adding a computer – this information normally does not become available to the Bit9 Server until the next scheduled cache upgrade. If you know you have made relevant changes or you see incorrect policy mapping, you can clear the server cache so that the Bit9 Server immediately begins updating AD information.

**To clear the server cache and update AD information:**

- On the Mappings tab of the Policies page, click **Clear Server Cache** in the Actions menu.

## Viewing AD Computer Details in the Bit9 Console

If you have integrated AD and Bit9 Server, anytime a computer name in an AD domain appears in a table in the Bit9 Console, additional information can be displayed by clicking on that computer name. For example, if you display the Events page, some events include the computer associated with the event.

If the name is an AD computer name, it should be highlighted in blue, and when you click on it, the Computer Details page appears. If you click the **AD Details** tab on this page the AD information that is available for that computer is displayed.

Similar information is displayed about a user when you click on a highlighted AD username in a console table.

## Downloading Agent Installers

When you create a new policy, the Bit9 Server generates a policy-specific agent installer for each agent platform and posts it to an agent download area. Each installer specifies the policy, policy settings, Enforcement Level, and the address of the server managing the agent.

When the Bit9 Server is upgraded, agent installers are also upgraded to the new version. Depending upon your upgrade plans, you might download the new agent version or allow the Bit9 Server to manage the upgrade. See “[Upgrading Bit9 Agents](#)” on page 119 for more details.

### Note

If you are using Active Directory to assign policies to all computers, use any installer whose policy has the *Automatic Policy Assignment for New Computers* box checked. Once the agent is installed on a computer and makes contact with the Bit9 Server, the correct AD-based policy for the computer will be assigned automatically. If the computer is unable to contact the Bit9 Server, the policy from the agent installer remains in effect.

Bit9 Agent installers are created in a file format appropriate for each platform:

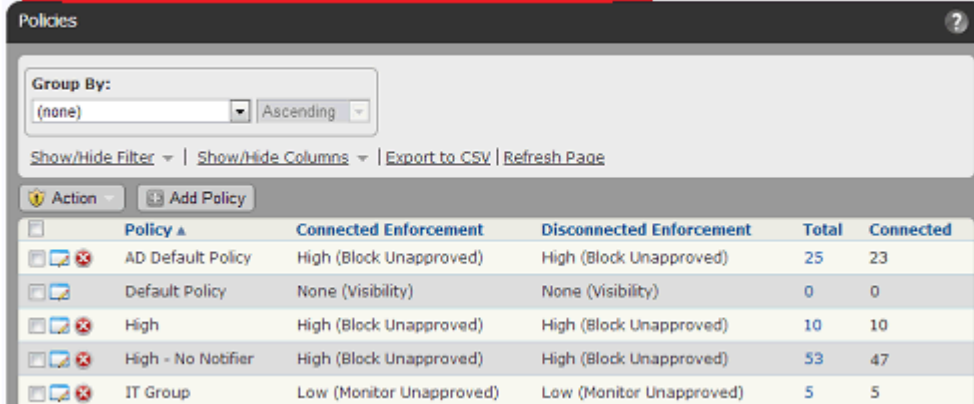
- MSI (Microsoft installer) packages for Windows
- DMG files for Mac OS X
- TGZ archives for Linux

The download page for these packages is accessible via a URL on the server. You can bookmark this URL and access the page without logging into the Bit9 Console.

### To download an agent installer:

1. In the console menu, choose **Rules > Policies**. The Policies page appears:

Users can download Bit9 Agent software from <https://bit9-1.mycorp.local/hostpkg>



The screenshot shows the Bit9 Policies page. At the top, a message states: "Users can download Bit9 Agent software from <https://bit9-1.mycorp.local/hostpkg>". Below this is a table with columns: Policy, Connected Enforcement, Disconnected Enforcement, Total, and Connected. The table lists several policies with their respective enforcement levels and counts.

Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
AD Default Policy	High (Block Unapproved)	High (Block Unapproved)	25	23
Default Policy	None (Visibility)	None (Visibility)	0	0
High	High (Block Unapproved)	High (Block Unapproved)	10	10
High - No Notifier	High (Block Unapproved)	High (Block Unapproved)	53	47
IT Group	Low (Monitor Unapproved)	Low (Monitor Unapproved)	5	5

2. From the Policies page, click the **download Bit9 Agent software** link. The publicly accessible URL for this page takes the following format:

`https://server_name/hostpkg`

The Download Install Packages page appears:

**Download Install Packages**

Bit9 Server protects your computer and the network from viruses, spyware, and other malicious applications.

Installing the Bit9 software is simple:

1. Click the installation setup file for the policy assigned to you by your network administrator.
2. Download the installation setup file to a convenient location on your hard-drive.
3. From the download directory, double-click the newly downloaded file to install Bit9.

Policy Name	Install Package	Description	Date Created ▲	Date Modified
Medium	Windows, Mac, Red Hat	Terminate banned files	Sep 30 2013 02:50:51 PM	Oct 3 2013 02:22:09 PM
Uninstall	Windows, Mac, Red Hat	Agent disabled	Sep 30 2013 02:51:10 PM	Oct 3 2013 02:22:11 PM
High	Windows, Mac, Red Hat		Sep 30 2013 02:51:33 PM	Oct 3 2013 02:22:13 PM
AD Default Policy	Windows, Mac, Red Hat		Oct 3 2013 04:28:07 PM	Oct 3 2013 04:28:09 PM
IT Group	Windows, Mac, Red Hat		Oct 3 2013 04:29:56 PM	Oct 3 2013 04:29:59 PM
High - No Notifier	Windows, Mac, Red Hat		Oct 3 2013 04:30:54 PM	Oct 3 2013 04:30:57 PM

6 items Page 1/1

3. In the Bit9 Installation Setup Files table, locate the installer file by policy name.
4. To download the installer, click the platform name (e.g, Mac) for the computer on which you want to install the agent, and save the file.
5. When the download is complete and you are read to install the agent, follow the instructions in the next section, [“Installing Bit9 Agents”](#).

## Installing Bit9 Agents

The Bit9 Agent installation process is non-interactive; it requires no user input. As soon as installation is completed, the Bit9 Agent begins working – no additional configuration or restart is needed.

### Preparing for New Agent Installation

*Before* installing a new Bit9 Agent on any platform, review the following:

- As soon as the Bit9 Agent is installed, the computer is protected by a security policy, and the agent connects with the server and begins initializing files. Because initialization can involve an increased flow of data between the Bit9 Server and its new client, be sure your agent rollout plans take your network capacity and number of files into account – simultaneous agent installation on all computers on a large network is not recommended.
- If you are configuring your Bit9 Server for the first time, consider setting up a reference computer with files you know you want to globally approve; you can also use that computer as a baseline for measuring any file inventory drift.
- Bit9 Agent is a per-system application, not per-user.
- Make sure the computer and operating system on which you are installing the agent is supported for the Bit9 Agent. See the separate *Operating Environment Requirements*

- document for the agent hardware requirements and *Supported Agent Operating Systems* for the OS versions on each platform supported by the current Bit9 Agent.
- Decide how the agent will be installed on this system. You can choose among the following options:
    - Use an existing software deployment mechanism. Although new agent installations are normally done in non-interactive mode, you can optionally create an interactive end-user installation experience. If you use a third-party distribution system to install Bit9 Agents, follow all recommended procedures. For Windows installations, disable any possible MSI or MSP transformations inside your distribution system (such as SCCM).
    - Have a system administrator or other qualified employee install the agent software manually on each user's computer.
    - Permit users to install the agent software themselves. Send e-mail to users associated with each policy and inform them to browse to the agent download URL or another shared location, download the specific installer file for their policy, and run the installation on their computers. No interaction is needed – the installation runs without prompts and then the agent begins to initialize files.
  - The Bit9 Agent installer must be run by a user with the appropriate administrative rights. On Windows, this can be either by Local System or by a user account that has administrative rights and a loadable user profile. On Mac and Linux, the user must be able to use *sudo*.
  - Be sure to download the correct installation package for your policy and platform; see [“Downloading Agent Installers”](#) on page 112. If you are using AD-based policy assignment, a platform-specific Bit9 Agent installer for any policy that allows automatic policy assignment may be used.
  - Although the console prevents creation of policies whose names have generally known invalid characters, examine the policy name to see whether it contains characters that might require special handling (such as escaping in a command line) on your specific platform.

## Installing the Agent on a Windows Computer

As an MSI package, the Bit9 Agent Windows installer can be customized as you choose, including modification of the installation directory. Please refer to the Microsoft MSI documentation for information about configuration options. The installer for Windows is named in the following way, varying by policy:

- *policyname.msi*

Bit9 Agent also makes use of MSP files for more efficient upgrade installations. See [“Upgrading Bit9 Agents”](#) on page 119.

### Notes

- The use of Windows Installer Transform files (.mst) is *not supported* with the Bit9 Agent installer on Windows clients.
- Bit9 Agent 7.2.1 cannot be installed on systems running Windows 2000, Windows 2003 Server versions prior to SP1, or Windows XP versions prior to SP2.

**To install a new Bit9 Agent on a Windows computer:**

1. On the client computer, run the Windows Bit9 Agent installer you have selected. You can use any of the standard means for installing from MSI files, with the following key considerations:
  - a. The default Bit9 Agent application directory is **C:\Program Files\Bit9\Parity Agent** for 32-bit systems and **C:\Program Files (X86)\Bit9\Parity Agent** for 64-bit systems. To change the installation directory, perform the installation from the command line using the appropriate MSI command-line options.
  - b. If you plan to accept the default application directory, you can use any MSI installation method, including simply double-clicking on the MSI filename.
2. During Windows agent installation, the Bit9 installer displays a message box that closes automatically when installation is complete. This box includes a Cancel button so you can end the installation before it completes, if necessary.
3. If you run anti-virus software, exclude the Bit9 installation directory from anti-virus scanning. For enhanced security, Bit9 self-protects its application directory. To avoid performance problems, use the mechanism provided by your AV software vendor to specify that the following files and directories are not scanned or blocked:
  - the Bit9 Agent process (**Parity.exe**)
  - the agent program directory (by default, **Program Files\Bit9** on 32-bit systems and **Program Files (x86)\Bit9** on 64-bit systems)
  - the agent data directory (by default, **ProgramData\Bit9\Parity Agent** on Vista, Windows 7 and Windows 2008 systems and **\Documents and Settings\All Users\Application Data\Bit9\Parity Agent** on other supported systems)
4. Personal firewalls such as Zone Alarm may recognize the Bit9 Agent as a new application and block access to the network. Instruct users running the Bit9 Agent to permanently allow it access on their computers.

See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for a description of what the user sees on a system protected by the Bit9 Agent.



### Important

- Changing the major or minor version of Windows after installing the agent is not supported, and doing so will produce health check failures and in some cases failure of the Windows upgrade. If you need to upgrade Windows or you see a health check failure that reports a mismatch between the agent and the build platform, contact Bit9 Technical Support for remediation recommendations. Service pack upgrades are fully supported and do not cause health check failures.
- If you are using DFS and have installed an agent on a Windows 2003 or XP system, you must reboot the agent system to get full enforcement of Bit9 file rules. Because of an operating system limitation, DFS operations (including file executions) cannot be detected by the Bit9 Agent until the system has been rebooted. In this case, and the Upgrade Status column on the Computers page shows Reboot Required for the affected computer.
- On any version of Windows, if a file is in use by another application when the Bit9 installer tries to write that file, the system schedules the file to be replaced on next reboot, and the console shows Reboot Required for the affected computer.

## Installing the Agent on a Mac Computer

For Mac computers, you install the Bit9 Agent by using the appropriate installer DMG file. Installers for Mac are named as follows, varying by policy:

- *polycyname-mac.dmg*

### Note

Bit9 supports installation of agents only on systems listed in the *Supported Agent Operating Systems* document for this release.

Download the correct agent installation package for your operating system and policy, as described in “[Downloading Agent Installers](#)” on page 112. If you are using AD-based policy assignment, an agent installer for any policy that allows automatic policy assignment may be used. The same downloaded agent installer can be used on multiple endpoints, and can also be distributed to endpoints via SSH or distribution mechanisms like Casper.

### To install a new Bit9 Agent on a Mac computer:

1. Open a Terminal window and change directory to the location where the installer was downloaded (by default, the user-specific Download directory).  

```
cd ~/Downloads
```
2. To begin the installation, double-click on the agent installation file you downloaded, *polycyname-mac.dmg*. A standard package installation dialog begins.
3. Respond to the installation dialog prompts, and when the dialog indicates the installation was successful, click **Close**. The agent begins operating immediately.



4. If you run anti-virus software, exclude the Bit9 installation directory from anti-virus scanning. For enhanced security, Bit9 self-protects its application directory. To avoid performance problems, use whatever mechanism is provided by your anti-virus software vendor to specify that the following directories are not scanned:
  - **/Applications/Bit9/Daemon/b9daemon** – the Bit Agent process
  - **/Applications/Bit9** – the Bit9 program directory
  - **/Library/Caches/com.bit9.agent** – the Bit9 data directory
  - **/Library/Extensions/b9kernel.kext** – the Bit9 driver location *for OS X versions 10.9 (Mavericks) and later*  
*-or-*  
**/System/Library/Extensions/b9kernel.kext** – the Bit9 driver location *for OS X versions prior to 10.9*
5. The Mac firewall may detect the Bit9 Agent as a new application and block access to the network. Instruct users to permanently allow incoming connections to **b9daemon**.

See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for a description of what the user sees on a system protected by the Bit9 Agent.

## Installing the Agent on a Linux Computer

For Linux computers, you install the Bit9 Agent by running a script after extracting the appropriate TGZ archive. Bit9 7.2.1 supports installation of agents on Linux computers running Red Hat and CentOS versions, both of which use the same installation file. The installation files are tarballs named in the following way, varying by policy and operating system:

- *policyname-redhat.tgz*

Bit9 recommends disabling Prelinking on RedHat and CentOS computers before installing agents. Prelinking has negative impacts on performance and Bit9 features (see the Release Notes). However, if you must enable Prelinking on your RedHat and CentOS systems, enable the RedHat Prelinking updater before installing agents. See [“Approving by Updater”](#) on page 246 for instructions on enabling updaters.

### Notes

- For Linux, Bit9 supports installation of agents only on those versions and kernels listed in the *Supported Agent Operating Systems* document for this release. Please also refer to the *Release Notes* for your version of the Bit9 Platform and agents for any special considerations.
- Although not required for the initial agent installation, **gawk** and **unzip** are required for Linux agent upgrades initiated by the Bit9 Server. If necessary, update the Linux distribution to include them before installing the agent.

The Bit9 Agent is normally installed with a GUI-based blocked file notifier. This notifier appears when a user attempts to take an action that is either totally blocked by Bit9 or that requires a user decision about allowing it to proceed. For Linux systems that are not

running a graphic interface package or prefer to eliminate user interaction for some other reason, the Bit9 Agent for Linux can be installed without the notifier. This `-n` option may be added as a flag on the installation script command for the agent, and is shown in the procedure below.

### Note

On a system that you choose to run without the notifier, you should install an agent with a Low or High Enforcement policy. Agents in Medium Enforcement policies prompt users to allow or block many actions, and this prompt will not be available without a notifier.

Download the correct agent installation package for your operating system and policy, as described in “[Downloading Agent Installers](#)”. For AD-based policy assignment, use an installer for any policy with automatic policy assignment enabled.

### To install a new Bit9 Agent on a Linux computer:

1. Make sure the account for the user installing the agent has administrative rights, or that the user can use **sudo**.
2. Extract and uncompress the agent tarball archive for the policy you have chosen for this computer. If the policy name contains characters not accepted in command arguments, such as spaces or parentheses, escape these characters with a backslash:  

```
tar -xvzf <policyname>-redhat.tgz
```
3. Change to directory matching the download tarball name.  

```
cd <policyname>-redhat
```
4. Use **sudo** to run the agent installation shell script using whatever shell you choose, adding the `-n` option if you do not want the blocked file notifier installed. For example, to use the Bourne shell to install an agent:  

```
sudo sh ./b9install.sh  
-or for installation without the notifier-  
sudo sh ./b9install.sh -n
```
5. If you run anti-virus software, exclude the Bit9 installation directory from anti-virus scanning. For enhanced security, Bit9 self-protects its own application directory. To avoid performance problems, use whatever mechanism is provided by your anti-virus software vendor to specify that the following directories or files are not scanned:
  - **/opt/bit9/bin** – the Bit9 Agent application and uninstall script
  - **/srv/bit9/data** – the Bit9 Agent database and diagnostics logs
  - **/lib/modules/kernelversion/kernel/lib/b9kernel.ko** – the Bit9 Agent kernel
  - **/etc/rc\*/b9daemon** and **/etc/init.d/b9daemon** – the Bit9 Agent startup script
  - **/etc/X11/xinit/xinitrc.d/90b9notifier.sh** – the Bit9 blocked file notifier
6. Firewalls may recognize Bit9 software as a new application and block access to the network. Instruct users running the Bit9 Agent to permanently allow it access.

See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for a description of what the user sees on a system protected by the Bit9 Agent.

## Verifying the Installation

To verify that connected computer is running the agent and visible to the server:

1. On the console menu, choose **Assets > Computers**.
2. Examine the Computers page, which lists all computers running agent software, for the name or IP address of each system you want to confirm. You can use the Search box to find each computer of interest.

Computer Name	Connected	Policy Status	Connected Enforcement	IP Address	Policy
MYCORP\DESKTOP-3	●	Up to date	High (Block Unapproved)	10.4.23.88	--Administration--
MYCORP\LAPTOP-6	○	Out of date	Medium (Prompt Unapproved)	10.4.11.107	--R&D Group--
MYCORP\DESKTOP4	●	Policy out of date	Medium (Prompt Unapproved)	10.4.11.24	--IT Group--

3. Note the computer's policy. If it was assigned by Active Directory, the policy will have dashes at the beginning and end of its name. Also note the Connected and Policy Status columns to determine whether the machine is up to date.

### Note

During file initialization for a newly installed agent, the computer is already protected at the Enforcement Level associated with its policy.

## Verifying Installation on the Agent Computer

You also can verify the presence of the Bit9 Agent locally on the agent computer:

- On Windows computers, open the **Task Manager** and click on the **Services** tab. You should see **B9Daemon** running.
- On Mac computers, run **Activity Monitor** and view **All Processes**. You should see **b9daemon** running.
- On Linux computers, use **ps aux | grep b9** in a command window. You should see **b9daemon** running.

## Upgrading Bit9 Agents

Bit9 Server upgrades also include new versions of the Bit9 Agent. There are several ways to upgrade the agent:

- Enable automatic agent upgrades on a per-policy basis, allowing the server to manage the upgrade process.
- Initiate agent upgrades on one or more specific computers from the Bit9 Console.
- Manually upgrade agents on the agent machine.
- Use your standard software distribution system to manage upgrades.

### Note

Server-driven Linux agent upgrades require that **gawk** and **unzip** are installed on the agent system. If they are not already installed, update the Linux distribution to include them before enabling or initiating agent upgrades.

## Feature Limitations for Non-Upgraded Agents

You can continue to run older Bit9 Agents, as long as they are at the 6.0 version level or greater, and are fully patched. However, you should upgrade your agents as soon as possible. Until a 6.x agent is upgraded, certain Bit9 Security Platform 7.2.1 features will not be fully functional or will use transitional functionality, including the following:

- **Custom Script Rules** will not work on pre-7.0 agents.
- **Custom Rules** that specify **write tracking exceptions** to write ignore rules will not work on pre-7.0 agents.
- The blocked file Notifier on computers running pre-7.0 agents does not include the **Approval Requests** feature, which allows users running 7.0 agents to submit a request for approval of the blocked file.
- **File reputation approvals** are not immediately effective on pre-7.0 agents. However, when any 7.0 agent requests access to a file with a reputation-based approval, Bit9 Server updates its approval list, and *all* agents (including pre-7.0) will receive that approval when their configuration list is updated by the server.
- **Publisher reputation approvals** are not available for pre-7.0. agents.
- Certain **Device Management Features** are not available for pre-7.0 agents. For example, you cannot ban a particular device type on a pre-7.0 agent. Also, detected devices on pre-7.0 agents appear in the Device Catalog (if unique) but do not appear on the Devices on Computers list. In addition, while 7.0 and later agents report *any* mounted device to the server, pre-7.0 agents report only those devices whose detection was supported in their Bit9 version, primarily USB devices and iPods (if filesystem detection is activated on the iPod).
- **Catalog-based (Detached Certificate) Publisher Approvals** are not available for files on pre-7.0 agents. As with reputation-based approvals, if a 7.0 agent accesses a file that is approved via catalog, that approval becomes available to pre-7.0 agents.
- Certain other **Certificate Management Features** are not available for pre-7.0.1 agents, including the ability to track, approve, and ban individual certificates.
- **Termination of Processes with Banned Images**, that is, the ability to configure a policy so that banned files are not only prevented from running but terminated if currently running, is not effective on pre-7.2 agents.
- Other performance and security enhancements are implemented in every release of the Bit9 Security Platform, and some of these will not be available on pre-7.2.1 agents.

The Bit9 Console displays a message when the presence of older agents affects the data shown or actions possible on a particular page.

## Enabling Automatic Agent Upgrades

During the Bit9 Server upgrade process, the flag that triggers the automatic agent upgrade process is set to “Disabled”. This allows the server upgrade to be verified prior to any agent upgrades on client computers. After you have upgraded the server, follow these steps to enable automatic upgrade of agents on systems connected to the server:

- For each policy whose agents you *do not* want to upgrade now, make sure the **Allow upgrades** box in the Options section of the Add/Edit Policy page is *not checked*.
- For each policy whose member agents you want to upgrade, check the **Allow upgrades** box in the Options section of the Add Policy or Edit Policy page.
- On the System Configuration/Advanced Options tab, check **Automatic Agent Upgrades**.

### Important

- Before you re-enable system-wide agent upgrades, be sure you *disable* upgrades for policies you don’t want upgraded immediately.
- Simultaneous upgrade of a large number of agents may impact system performance. Contact Bit9 Support for best practices for bulk agent upgrades.
- When Bit9 Server is upgraded from one major version to another (such as v6.0.2 to v7.2.1), ongoing enhancements to “interesting” file identification make it necessary to rescan the fixed drives on all agent-managed computers. These upgrades also require a new inventory of files in any trusted directories to determine whether there are previously ignored files that are now considered interesting. This process involves the same activity as agent initialization, and can cause considerable input/output activity, which can require between minutes and many hours, depending upon the number of agents and the number of files.

For both upgrades managed by the Bit9 Server and those using third-party distribution methods, Bit9 recommends a gradual upgrade of agents to avoid an unacceptable impact on network and server performance.

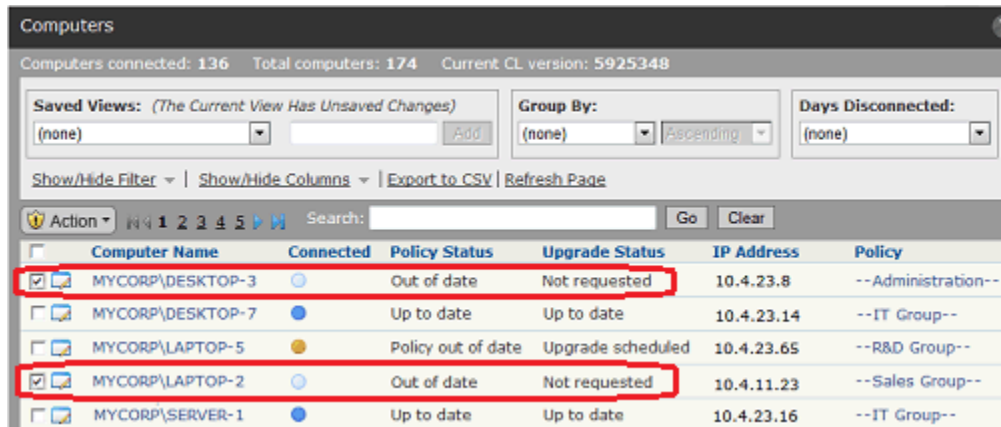
## Upgrading Immediately from the Bit9 Console

In the Bit9 Console, you can *enable* automatic agent upgrades to happen as part of the Bit9 Server’s regular maintenance of computers, but you can also *force* upgrade of an agent through the console. This has the same effect as running the upgrade from the installer (or for Windows, the upgrade MSP) file. Use of this feature requires the following:

- Automatic Agent Upgrades must be Enabled on the Advanced Options tab of the System Administration page. The Upgrade Computers choice does not appear on the menu unless this is enabled.
- The agents(s) must be at least at version 6.0.0 – upgrades from older agents are not supported.

**To immediately upgrade one or more agents from the console:**

1. On the console, choose **Administration > System Configuration** and then click on the **Advanced Options** tab.
2. On the Advanced Options tab, if the Automatic Agent Upgrades field is *Disabled*, click the **Edit** button, choose **Enabled** from the Automatic Agent Upgrades menu, and then click **Update** to make the change.
3. On the console menu, choose **Assets > Computers**.
4. Find the computer(s) you want to upgrade and check the checkboxes next to their names. Check the Upgrade Status to make sure the computers are capable of upgrade and not already up to date.



5. In the Action menu, select the **Upgrade Computers** command.



6. In the confirmation dialog, click **OK** to trigger the upgrade. Watch the description of the computer in the table to see when the change is completed.

**Note**  
 Agents disconnected from Bit9 Server at the time of a console-based “immediate” upgrade will be upgraded the next time they are connected.

## Manually Upgrading Agents

For disconnected systems or if you are using a software distribution system such as SCCM or Altiris to distribute upgrades, you will have to distribute Bit9 Agent installation files to the endpoints or distribution server.

Installation files for Bit9 Agent are located on the Bit9 Server in **Program Files\Bit9\Parity Server\hostpkg** on 32-bit systems and **Program Files (x86)\Bit9\Parity Server\hostpkg** on 64-bit systems.

## Manually Upgrading Windows Agents

There are different files for upgrading Windows agents depending upon what version of the agent you currently are running:

- Use **ParityHostAgent.msi** to upgrade from a pre-7.0 agent, and for upgrades from 7.0.0, 7.0.1, and 7.2.0 agents. You must also download **configlist.xml** from the **hostpkg** folder to assure agent protection immediately after upgrade.
- **ParityAgent7.2.1.msp** is for use only when Bit9 Technical Support informs you that you should install a build-to-build upgrade (“patch”) of the same release; i.e., the three-part version number is the same (e.g., upgrading from 7.2.1.434 to 7.2.1.568). This msp should not be used for upgrades if any of the first three parts of the version number are different (e.g., upgrading from 7.0.1 to 7.2.1).

### Important

- Manual upgrades must be run either by Local System or by a user account that has administrative rights and a loadable user profile.
- Manual upgrades from 6.0.x agents to 7.2.1 agents must use a full path to the installer in the MSIEXEC command. Upgrades from the 7.0.x agent will not require the path.

When a Bit9 Server manages upgrades to v7.2.1 agents, the agents receive a new list of rules. For manual agent upgrades and upgrades using a third-party distribution method, the file containing the new rules, **configlist.xml**, must be copied to a location accessible to the agent installer. On the Bit9 Server, the **configlist.xml** file is located in the same **hostpkg** folder as the agent installer, but it must be manually copied or referenced with a URL or path in the installer.

### To upgrade a Windows agent manually or via third-party mechanisms:

1. Log in to the Bit9 Console on the computer to which you want to download the installer.
2. On the console menu, choose **Rules > Policies** and click on the download agent software link at the top of the Policies page
3. Download the Bit9 Agent upgrade installer file appropriate for your situation to the location from which you want to run or distribute the upgrade:
  - To upgrade from any supported pre-7.2.1 version, download **ParityHostAgent.msi**.
  - To upgrade from a different build of 7.2.1, download **ParityAgent7.2.1.msp**.

You can do this by using a URL, UNC path, or any other standard means getting to the file. Note that this installer is not listed on the Downloads page in the Bit9 Console.

To use a URL, you can choose **Rules > Policies** in the console, click on the Download link at the top of the page, and edit the URL for the download page as follows:

**https://<bit9servername>/hostpkg/pkg.php?pkg=<installerfile>**

4. Choose the Save option provided by your browser.

5. Follow the same procedure to download the Bit9 Security Platform 7.2.1 rules list **configlist.xml** to a location accessible to the agent installer, or make sure the agent installer system has access to the *hostpkg* folder on the Bit9 Server. To use a URL, you would enter the following on a browser on the computer to which you want to download the file:

**https://<bit9servername>/hostpkg/pkg.php?pkg=configlist.xml**

**Note:** If you are using a command line argument to upgrade the agent, you do not necessarily have to *download* configlist.xml. You can use the URL above as an argument in the command line. See Step 7.

6. If you are upgrading a single computer manually, move the configlist.xml file to the Bit9 Agent data folder, usually **C:\ProgramData\Bit9\Parity Agent**, and then run the installer, for example, **ParityHostAgent.msi**.
7. If you are preparing to upgrade agents via a third-party distribution system, you can use that system to distribute the configlist.xml file to the agent folder on all agents, or you can use command line arguments in MSIEXEC to include the new rules file in the upgrade installations. A command line for such an upgrade using ParityHostAgent.msi might look like the following:

```
msiexec /i <path>\ParityHostAgent.msi B9_CONFIG=  
https://<bit9serverIP>/hostpkg/pkg.php?pkg=  
configlist.xml /L*v+ c:\ParityHostAgentUpgrade.log
```

Note that you can use a URL, a UNC path, or a full local path to specify the location of configlist.xml in the command. You cannot use a relative path or a file name without a path.

## Manually Upgrading Mac Agents

Once the Bit9 Server has been upgraded, you can download and manually upgrade a v7.2.0 or later Mac agent to a newer version

### Note

Manual upgrades from v7.0.1 agents to v7.2.1 agents are not supported. If you are upgrading from v7.0.1 and cannot use a server-managed upgrade method, uninstall the v7.0.1 agent and then install a new v7.2.1 agent.

### To upgrade a 7.2.0 or later Mac agent manually:

1. Either disable Tamper Protection for the agent or put the agent into a Disabled mode policy.
2. In the Bit9 Console, choose **Rules > Policies** and click on the download agent software link at the top of the Policies page.
3. Download the upgrade installer for Mac agents, which is **Bit9MacInstall.bsx**.

You can do this by using a URL, UNC path, or any other standard means getting to the file. Note that this installer is not listed on the Downloads page in the Bit9 Console.



To use a URL, you can choose **Rules > Policies** in the console, click on the Download link at the top of the page, and edit the URL for the download page as follows:

```
https://<bit9serverIPAddress>/hostpkg/pkg.php?pkg=Bit9MacInstall.bsx
```

4. Open a Terminal window and change directory to the location where the installer was downloaded (by default, the user-specific Download directory).

```
cd ~/Downloads
```

5. Enter the following command to install the agent:

```
sudo bash Bit9MacInstall.bsx
```

## Manually Upgrading Linux Agents

Once the Bit9 Server has been upgraded, you can download and install an upgraded Bit9 Agent on a Linux system. For most endpoints, you should also download and run the notifier upgrade installer.

### To upgrade a Linux agent manually:

1. Either disable Tamper Protection for the agent or put the agent into a Disabled mode policy.
2. In the Bit9 Console, choose **Rules > Policies** and click on the download agent software link at the top of the Policies page.
3. Download the agent upgrade installer for the Linux, **bit9redhat6install.bsx** or **bit9redhat6install.bsx**, to the client computer.

This installer is not listed on the Downloads page in the Bit9 Console. You can download it using a URL, UNC path, or any other standard file address syntax. To use a URL, you can choose **Rules > Policies** in the console, click on the Download link at the top of the page, and edit the URL for the download page as follows:

```
https://<bit9servername>/hostpkg/pkg.php?pkg=bit9redhat{6,7}install.bsx
```

4. Run the agent upgrade installer on the client computer from the command line.

```
sudo bash -U bit9redhat{6,7}install.bsx
```

## Agent Upgrade Status

To make the upgrade process easier to manage, the Computers page in the Bit9 Console provides an Upgrade Status column and also visually differentiates between computers running up-to-date agents and those running previous versions. On this page, computers running *previous* agent versions show an orange dot in the “Connected” column while up-to-date agents are shown with a blue dot.

Computer Name	Connected	Policy Status	Upgrade Status	IP Address	Policy
MYCORP\DESKTOP-3	○	Out of date	Not supported	10.4.23.8	--Administration--
MYCORP\DESKTOP-7	●	Up to date	Up to date	10.4.23.14	--IT Group--
MYCORP\LAPTOP-5	●	Policy out of date	Upgrade scheduled	10.4.23.65	--R&D Group--
MYCORP\LAPTOP-2	○	Out of date	Not requested	10.4.11.23	--Sales Group--
MYCORP\SERVER-1	●	Up to date	Up to date	10.4.23.16	--IT Group--

In addition, the Upgrade Status column in the Computers table shows a more detailed description of agent status as each agent goes through the upgrade process. Clients will transition to an Upgrade Status and Policy Status of “Up to Date” when all their upgrade processing has been completed. Table 13 shows the possible Upgrade Status values.

**Note**

An upgraded Bit9 Agent begins running immediately. You usually do not need to reboot the agent computer, but there are cases in which you may see an Upgrade Status is “Reboot Required”:

- Some Windows XP/2003 systems must be rebooted after upgrade to assure proper ordering of processes and enforcement of rules on systems using DFS.
- On any Windows version, if a file is in use by another process when the agent installer attempts to write that file, you must reboot the computer to allow the system to replace the old file with the current version.

**Table 13:** Upgrade Status Messages

Upgrade Status	Description
<b>Not Requested</b>	Agent can be upgraded but upgrades are not enabled for the policy, or they are turned off globally.
<b>Upgrade waiting</b>	Agent can be upgraded and is in a policy that allows upgrade. Waiting to be scheduled by server.
<b>Upgrade scheduled</b>	Agent has been scheduled for upgrade, or computer has downloaded the upgrade package and not run it yet. Note that the server does not track <i>when</i> the agent upgrade package is downloaded and run.
<b>Upgrade requested</b>	An agent upgrade for this computer was requested from the Bit9 Console.
<b>Reboot required</b>	Agent is waiting for a reboot after upgrade. Reboot is required only under certain conditions (see note above).

Upgrade Status	Description
<b>Not supported</b>	Agent cannot be upgraded because the computer is running Windows 2000 or another operating system not supported for 7.2.
<b>Upgrade blocked</b>	Agent configuration list is not up-to-date and is missing one or more values required for a successful upgrade. One example of this is use of an out-of-date port number for communication with the Bit9 Server. Agent cannot upgrade through the server until the configuration is up-to-date, but can be upgraded through other means. In most cases, a connected agent will eventually reach the required configuration list version without intervention. Prioritizing the agent for updates (on the Computer Details page Action menu) expedites configuration list updates. If an agent still remains in "Upgrade blocked" for an extended period, contact Bit9 Technical Support.
<b>Up to date</b>	Agent upgrade (or new installation) has been completed.
<b>Agent uninstalled</b>	Agent was on this computer but has been uninstalled.

## Uninstalling Bit9 Agents

Standard un-installation procedures delete all Bit9 files, including the notifier program and drivers. Computer users are not permitted to uninstall an enabled Bit9 Agent unless they have special agent administrative access as described in [“Configuring Agent Management Privileges”](#) on page 615.

To uninstall, you must disable the Bit9 Agent by placing the computer in a policy that is in Disabled mode, which can be done on the Computers page. If you have not already done so, log in to the Bit9 Console and create a policy with its Mode set to **Disabled** before attempting to uninstall any agents. If you create a policy for uninstallation purposes (which you could name “agent disabled policy,” for example), the server automatically creates an agent installer for it and adds the installer to the list on the Download Install Packages page.

### Uninstalling the Agent from a Windows Computer

#### To uninstall the Bit9 Agent:

1. From the Bit9 Console, find the computer on the Computers page and move it into the agent disabled policy.
2. On the client computer, shut down all other applications.
3. On the client computer, run the standard program removal procedure from the Windows Control Panel:
  - a. On the Windows Control Panel, choose **Add or Remove Programs**, or for Vista or Windows 7 systems, **Programs and Features**.
  - b. From the list of programs, select **Bit9 Agent**.
  - c. Click the **Remove** button or **Uninstall** button (depending upon your operating system) and wait for the uninstall to complete.

4. Delete the computer from the Computers page in the Bit9 Console. This tells the Bit9 Server that the computer is no longer in service (rather than temporarily disconnected from the network) and removes its name from the table of active computers.

## Uninstalling the Agent from a Mac Computer

1. From the Bit9 Console, move the computer into the agent disabled policy.
2. In a Terminal or another shell interface, run the following command:

```
sudo /Applications/Bit9/uninstall.sh
```

The Bit9 Agent and its data are removed.

3. Delete the computer from the Computers page in the Bit9 Console. This indicates to the Bit9 Server that the computer is no longer in service rather than temporarily disconnected from the network) and removes its name from the table of active computers.

## Uninstalling the Agent from a Linux Computer

1. From the Bit9 Console, move the computer into the agent disabled policy.
2. On the client computer, login with administrator privileges or an account that can run sudo.
3. In a shell window, change to the Bit9 Agent application directory:

```
- cd /opt/bit9/bin
```

4. Run the uninstall script:

- To remove the agent and all of its data:

```
sudo sh ./b9uninstall.sh
```

- To remove the agent but preserve Bit9 Agent data in **/srv/bit9**:

```
sudo sh ./b9uninstall.sh -d
```

5. Delete the computer from the Computers page in the console. This indicates to the Bit9 Server that the computer is no longer in service (rather than temporarily disconnected from the network) and removes its name from the table of active computers.

## Viewing the Table of Computers

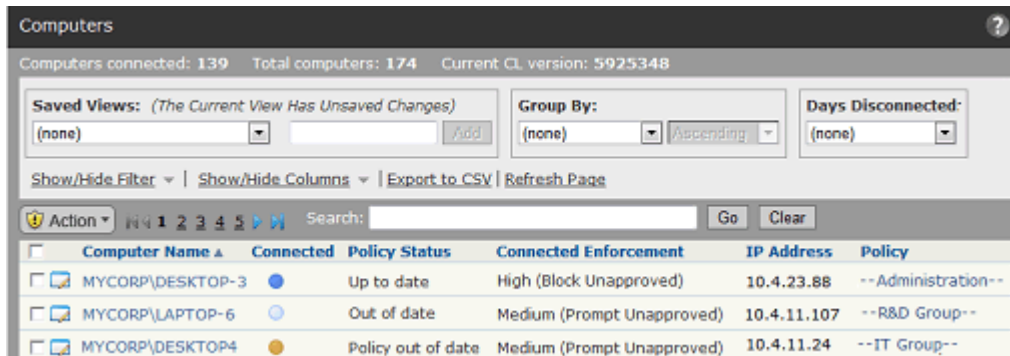
On the Computers page, you can view a table of computers and information about them, including their platform, policies, Enforcement Levels, and whether they are currently connected to the server. As with most console tables, you can add or remove details in the visible table using the Columns button. You also can use the Search field to narrow down the computers listed on the page to those you are most interested in. For more information on customizing your view, see [Bit9 Console Tables](#) in [Chapter 2, “Using the Bit9 Console.”](#)

In addition to the table of agent-managed computers, the Computers page shows the following information:

- **Computers connected** – Shows the number of computers running the Bit9 Agent that are currently connected to the server.
- **Total computers** – Shows the total number of computers that are currently members of security policies managed by the server.
- **Current CL version** – Shows the version number of the latest Configuration List (CL) available from the server. This can be used to help determine whether the CL for a particular agent is out of date. Note, however, that some CL versions are agent-specific, so the fact that the CL version for an agent doesn't exactly match the CL version shown here does not automatically mean the agent is out of date.

**To view the table of computers managed by your Bit9 Server:**

1. In the console menu, choose **Assets > Computers**. The Computers page appears:



Computer Name	Connected	Policy Status	Connected Enforcement	IP Address	Policy
MYCORP\DESKTOP-3	●	Up to date	High (Block Unapproved)	10.4.23.88	-- Administration --
MYCORP\LAPTOP-6	○	Out of date	Medium (Prompt Unapproved)	10.4.11.107	-- R&D Group --
MYCORP\DESKTOP4	○	Policy out of date	Medium (Prompt Unapproved)	10.4.11.24	-- IT Group --

2. The Search field provides a way to search for computers by name (or partial name), IP Address, or Policy to reduce the length of the Computers table and help you find the systems you want. You enter the string you want to match against computer names and then click **Go**. Click **Clear** to restore the list of computers that appeared prior to the search.
3. Saved Views provide another way to limit the Computers table to systems matching certain characteristics:
  - Choose **Carbon Black Deployments** to see computers grouped by whether they have had a Carbon Black agent installed on them.
  - Choose **Cloned Computers** to see computers that have been cloned from a template computer. See [Chapter 6, “Managing Virtual Machines,”](#) for details.
  - Choose **Computers in Local Approval** to see previously locked down computers that have received approval from the server to install software in Local Approval mode.
  - Choose **Computers Requiring Upgrade** to see computers running Bit9 Agents that are not up to the current version.
  - Choose **Connected Computers** to see only computers running Bit9 Agents that are currently connected to the server.
  - Choose **Disconnected Computers** to see computers running Bit9 Agents that are not currently connected to the server.
  - Choose **Duplicate Computers** to see computers that have the same name as other computers in your Bit9 database. See [“Duplicate Computers”](#) on page 147 for details.

- Choose **Template Computers** to see computers that are templates for cloned computers. See [Chapter 6, “Managing Virtual Machines,”](#) for details.
  - Choose **(none)** to return to the complete list of computers managed by this server.
  - Other Saved Views may be available if you or another console user created them.
4. You can click on **Show/Hide Filter** and/or **Show/Hide Columns** to open the Filters and Columns interface, which let you further customize the view you have of the Computers table.

[Table 15](#) provides descriptions of the fields available on the Computer Details page, most of which are also available in the Computers table, either by default or by customization.

## Agent Policy Status

The Computers table includes a column called “Policy Status,” which indicates whether the agent for each listed computer is up to date with the Bit9 Server rules that should apply to it. Note that this field does not appear on the Computer Details page.

### Note

During system initialization, the computer is already protected at the Enforcement Level associated with its security policy.

The screenshot shows the Bit9 console interface for the 'Computers' table. At the top, it displays 'Computers connected: 136', 'Total computers: 174', and 'Current CL version: 5925348'. Below this are controls for 'Saved Views', 'Group By', and 'Days Disconnected'. The main table has columns for 'Computer Name', 'Connected', 'Policy Status', 'Upgrade Status', 'IP Address', and 'Policy'. The 'Policy Status' column is circled in red, showing values: 'Out of date', 'Up to date', 'Policy out of date', 'Out of date', and 'Up to date'.

Computer Name	Connected	Policy Status	Upgrade Status	IP Address	Policy
MYCORP\DESKTOP-3	●	Out of date	Not supported	10.4.23.8	--Administration--
MYCORP\DESKTOP-7	●	Up to date	Up to date	10.4.23.14	--IT Group--
MYCORP\LAPTOP-5	●	Policy out of date	Upgrade scheduled	10.4.23.65	--R&D Group--
MYCORP\LAPTOP-2	●	Out of date	Not requested	10.4.11.23	--Sales Group--
MYCORP\SERVER-1	●	Up to date	Up to date	10.4.23.16	--IT Group--

[Table 14](#) shows the possible values of Policy Status.

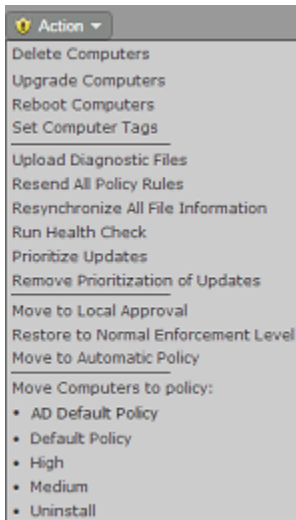
**Table 14:** Policy Status Messages

Policy Status	Description
<b>Up to date</b>	Agent Enforcement Level, policy, and rules are all up to date.
<b>Policy out of date</b>	Agent is not up to date on changes to its policy.
<b>Approvals out of date</b>	Agent rules (including file approvals or bans, trusted users, publisher rules, updater rules, device rules, memory rules and registry rules) are out of date.

Policy Status	Description
<b>Enforcement Level out of date</b>	Agent Enforcement Level is out of date.
<b>Out of date</b>	Agent is out of date on more than one of these: Enforcement Level, policy, or rules.

## Actions on Selected Computers

The Action menu on the Computers page provides commands that can be applied to one or more computers. You select computers to be acted on by checking the box to the left of their row.



The actions include deleting, upgrading, tagging, and rebooting computers, and moving the computers to different policies. Additional commands available on this menu are described in the Actions and Advanced sections of [Table 17, “Computer Details page menus”](#), on page 139.

## Viewing Complete Details for One Computer

There are several ways to locate a computer and display its details. You can use the Find Computer portlet on the Home Page to locate the computer and then drill down to its details. The following procedure describes how you can locate and get details for a computer through the Computers page.

### Note

If the computer for which you request details is a Template Computer, clicking the View Details button shows a Template Details page, not a Computer Details page. See [Chapter 6, “Managing Virtual Machines,”](#) for more information.

### To view the Computer Details page for a computer:

1. In the console menu bar, choose **Assets > Computers**. The Computers Page appears.
2. In the Computers table, locate the computer for which you want complete details (for example, using the Computer filters panel).
3. In the table, click either the name of the computer or the View Details button next to its name. The Computer Details page appears:

**Computer Details**

**General**

Computer Name: MYCORP\Server-4  
 IP Address: fe20::8cc:9ccc:3120:2812  
 Connection Status: Connected  
 Health Check: Passed  
 Platform: Windows  
 Description:   
 Computer Tag:

**Policy**

Policy: Medium  
 Policy Mode: Control  
 Connected Enforcement: Medium (Prompt Unapproved)  
 Disconnected Enforcement: Medium (Prompt Unapproved)

**Bit9 Agent** | Connection History | Policy Override | System Details | AD Details | Carbon Black

CLI Password: PRTY-ATPE-INTO-GWRW  
 CL Version: 1148  
 Debug Level: None (default)  
 Bit9 Agent Version: 7.2.0.181  
 Enabled Trusted Directories: 0  
 Tamper Protect: Enabled

**Related Views**

- Recent Events
- Health Check Events
- Files on this Computer
- Carbon Black Details

**Actions**

- Change Policy
- Delete Computer
- Prioritize Updates
- Add Files to Snapshot

**Advanced**

- Convert to Template
- Set Debug Level
- Configure Agent Dumps
- Reset CLI Password
- Disable Tamper Protection
- Change Local State
- Perform Cache Consistency Check
- Other Actions

4. The General and Policy sections of the Computer Details page appear in all views. The bottom panel on the page varies depending upon the tab you click:
  - Click **Bit9 Agent** (the default, shown above) to view version, password, and other configuration information for the agent on the Computer whose details you are viewing.



- Click **Connection History** to see the status of the agent's communication with the Bit9 Server, including whether it fully initialized and synchronized with the server ("Synchronized" appears only after initialization is complete).

Bit9 Agent | Connection History | Policy Override | System Details | AD Details | Carbon Black

**First Registered:** Apr 4 2014 01:29:05 PM  
**Last Polled:** Apr 7 2014 12:24:53 PM  
**Last Register Date:** Apr 7 2014 09:29:27 AM  
**Initialization:** Complete  
**Synchronization:** 100%  
**Server Backlog:** 0 files  
**Last Logged In User(s):** MYCORP\SERVER-4\$  
 MYCORP\rjones

- Click **Policy Override** to generate an override code that can be used to temporarily reassign the agent to a different Enforcement Level.

Bit9 Agent | Connection History | Policy Override | System Details | AD Details | Carbon Black

**Temporary Enforcement:** Local Approval  
**Enforcement Level Active For:** 30 Minute(s) (up to 500)  
**Code Valid For:** 5 Minute(s)  
 Generate Code

- Click **System Details** to get any available information about the CPU, memory, and operating system of the computer.

Bit9 Agent | Connection History | Policy Override | System Details | AD Details | Carbon Black

**Computer Model:** Latitude E5420  
**Processor:** Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz, 4 CPUs, 2.10 GHz  
**Installed Memory:** 3.25 GB  
**Operating System:** Microsoft Windows 7 x86 Service Pack 1 (build 7601)  
**Virtualized:** No

- Click **AD Details** to see any information Active Directory provides about this computer (only available if you have AD integration activated).

Bit9 Agent | Connection History | Policy Override | System Details | AD Details | Carbon Black

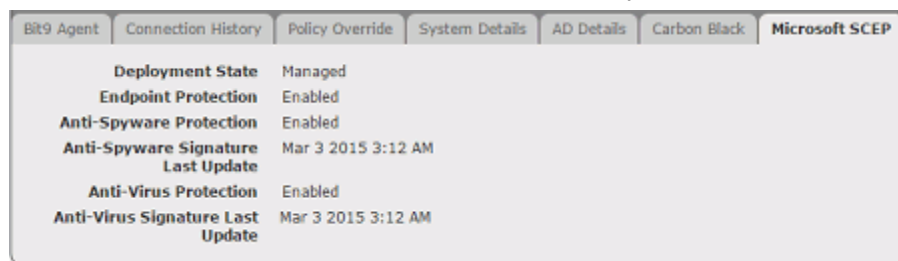
**Distinguished Name:** CN=SERVER-4,OU=Servers,DC=mycorp,DC=local

- Click **Carbon Black** to see details reported about this computer by the Carbon Black server configured on the Bit9 System Configuration page Licensing tab. If a Carbon Black server is not configured or the computer is not running a Carbon Black sensor, this tab shows only a status of *Not installed*. By default, the Bit9 Server checks Carbon Black status every 30 minutes.

Bit9 Agent | Connection History | Policy Override | System Details | AD Details | Carbon Black

**Sensor Version:** 4.2.0.40325  
**Last Status:** Running  
**Uptime:** 118 minutes(s)  
**Computer Status:** Online  
**Registration Time:** Apr 07 2014 02:18:48 PM  
**Last Checkin:** Apr 07 2014 04:16:49 PM  
**Next Checkin:** Apr 07 2014 04:17:19 PM  
[More information](#)

- Click **Microsoft SCEP** to see the status of Microsoft SCEP protection on this computer. This tab appears only if SCEP is integrated with the Bit9 Server. By default, the Bit9 Server checks SCEP status every 60 seconds.



**Table 15:** Computer Details (Details page and Computers table)

Field	Description
<b>Computer name</b>	Network name for the computer.
<b>IP address</b>	IP address for the computer. This may be an IPv4 or IPv6 address – if the Bit9 Server is configured for IPv6, Bit9 Agents will attempt to connect via IPv6 first.
<b>Identifier</b>	MAC address for the computer. (Option in table only)
<b>Connection status</b>	<p>Status of computer’s communication with the Bit9 Server:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b> – in communication with the Bit9 Server.</li> <li>• <b>Disconnected</b> – not communicating with the Bit9 Server.</li> </ul> <p>The Computers table also includes a circle icon in the Connection status field that indicates connection and agent status:</p> <ul style="list-style-type: none"> <li>● (Blue) – Connected, up to date</li> <li>● (Light Blue) – Disconnected, up to date</li> <li>● (Solid Orange) – Connected, unsupported (agent out of date or requires reboot)</li> <li>○ (Clear with Gray Border) – Template computer</li> <li>● (Red) – Connected, health check failed; indicates that the agent needs immediate attention. Collect the Health Check Events for this computer and contact Bit9 Technical Support.</li> </ul>
<b>Health Check</b>	<p>Agent health status. The health check includes a series of tests to see whether the agent is working properly. If the value is Passed, there are no known health issues with the agent on this computer. If the value is Failed, there is an issue with at least one aspect of agent health. In this case, click Health Check Events on the Computers Details page and contact Bit9 Technical Support.</p> <p><b>Note:</b> Health checks run automatically, but if you have addressed an agent problem and want to be sure the agent is healthy, you can force a health check using the <b>Run health check</b> command on the Other Actions menu of the Computer Details page.</p>
<b>Platform</b>	The basic operating system platform of this computer. Possible values are Windows, Mac, and Linux. The System Details tab of the Computer Details page shows additional detail.

Field	Description
<b>Days Offline</b>	If a computer is disconnected, adding this column to the Computers table shows how long it has been disconnected, and allows filtering by number of days.
<b>Upgrade status</b>	Agent upgrade status of this computer. See <a href="#">“Agent Upgrade Status”</a> on page 125 for status options. On the Computer Details page, only appears for computers requiring upgrade.
<b>Upgrade error time</b>	If an error occurred on agent upgrade, the time of that error. On the Computer Details page, only appears for computers on which an upgrade was attempted.
<b>Policy status</b>	Status (up-to-date or not, etc.) for the policy protection of this computer. See <a href="#">“Agent Policy Status”</a> on page 130 for details.
<b>Description</b>	Optional information about this computer, displayed on the Computer Details page. When entering or editing this text on the details page, click the <b>Update Computer</b> button to save.
<b>Computer tag</b>	Optional text string you can add to identify groups of computers that you might want to get reports about or treat in a particular way. A tag offers an alternative to policies as a way to identify groups of computers. For example, you might want to apply a Low (Monitor Unapproved) policy to all computers in your office but be able to track file activity in more specific reports for computers in tagged subgroups such as sales or accounting.  Tags may be set on the Computer Details page for one computer or on the Computers page Action menu for multiple computers.
<b>Policy</b>	Currently assigned policy for the computer.
<b>Policy Mode</b>	Security mode in which this policy is operating. The choices are Visibility, Control, and Disabled.
<b>Connected Enforcement</b>	Assigned Enforcement Level while the computer is in communication with the Bit9 Server. To change this setting for this computer and its fellow policy members, edit the policy. If the Enforcement Level is not up to date with changes to the policy on the server, “(out of date)” will be appended.
<b>Virtualized</b>	Indicates whether this computer is a virtual machine (Yes, No). On the Computer Details page, this is combined with Virtual Platform into a single field on the System Details tab.
<b>Virtual Platform</b>	If this is a virtual machine, the virtualization platform used to generate it. Current values are blank, VMware, and Unknown. On the Computer Details page, this is combined with Virtualized into a single field on the System Details tab.
<b>Clone Inventory</b>	If this is a template used to create clones, shows whether the inventory for clones created from this template includes All Files (including those from the template image) or just New and Modified Files (since creation of each clone). Field is blank for non-template computers. See <a href="#">Chapter 6, “Managing Virtual Machines,”</a> for more details.

Field	Description
<b>Inventory</b>	If this is a virtual machine, shows whether the inventory for this clone includes All Files (including those from the template image) or just New and Modified Files (since creation of this clone). Field is blank for non-clone computers. See <a href="#">Chapter 6, “Managing Virtual Machines,”</a> for more details.
<b>SCEP Status</b>	If Microsoft SCEP is integrated with this Bit9 Server, shows the status of the SCEP agent on this computer. The values are: <ul style="list-style-type: none"> <li>• Unknown – SCEP integration is not enabled.</li> <li>• Not Present – SCEP agent is not installed on this computer.</li> <li>• Disabled – One or both SCEP agent components is disabled.</li> <li>• Outdated – SCEP is installed but the signatures for one or both components is older than 3 days.</li> <li>• Active. – SCEP is installed and enabled for both components, and all signatures are up to date.</li> </ul>
<b>Save</b> (button)	Applies changes made to the Description and Computer tag in the General panel of the Computer Details page.
<b>Cancel</b> (button)	Clears unsaved changes made to the Description and Computer tag if you click it before you click the <b>Save</b> button. Page reverts to the settings in effect before you began editing.

**Table 16:** Computer Details page: Tabbed sections

Field	Description
<b>Bit9 Agent tab</b>	
<b>CLI Password</b> ( <b>CLI Code</b> in table)	Code that can be used to enable a command-line diagnostic utility for the Bit9 Agent installed on this computer. Reserved for use by Bit9 Technical Support representatives.
<b>CL Version</b>	Configuration List version number used to determine computer synchronization with server rules. If not the latest, “(out of date)” appears with the number. You can compare the CL version for a particular computer with the current CL version for the Bit9 Server, which appears on the Computers page. Also, the details page for many Bit9 Security Platform rules shows the CL version in which the current definition of the rule was introduced. For use with Bit9 Support.
<b>Debug Level</b> ( <b>Agent Debug Level</b> in table)	Shows current debug level for this agent, which indicates the amount of debugging information collected from it. This can be changed on the Advanced menu. For use with Bit9 Support.
<b>Bit9 Agent Version</b>	Version number of the Bit9 Agent installed on this computer.
<b>Enabled Trusted Directories</b>	The number of Trusted Directories currently enabled on this computer. See <a href="#">“Approving by Trusted Directory”</a> on page 228 for more information.
<b>Tamper Protect</b>	Status of agent tamper protection features. Value is either Enabled or Disabled.
<b>Connection History tab</b>	

Field	Description
<b>First Registered</b>	Date and time this computer first registered with the Bit9 Server.
<b>Last Polled</b>	Date and time this agent last polled the Bit9 Server for updated information and provided updated file information to the server. Agents may poll every 30 seconds, or as seldom as every 10 minutes if the agent is in "sleep" state because the server has no new information about policy changes, approvals, etc.
<b>Last Register Date</b>	Date and time the agent last connected to the Bit9 Server.
<b>Synchronization</b> (%Synchronization in table)	Percent of synchronization of file information between this agent and its Bit9 Server. Appears only after initialization is complete.
<b>Initialization</b> (% Initialization in table)	During initialization, shows the percent of initialization that is complete. Shows as "Complete" after initialization reaches 100%.
<b>Server Backlog</b>	The number of files received from this computer but not yet fully processed on the server. Backlogged files appear in the File Catalog but not in the Files on Computers tab or Find Files page.
<b>Last logged in user(s)</b>	User(s) logged in when the computer last connected to the Bit9 Server. If AD integration is enabled, click this field for more information about the user.
<b>Policy Override tab</b>	Allows generation of a code to temporarily change the Enforcement Level of a disconnected computer. See <a href="#">"Using Timed Policy Overrides"</a> on page 262.
<b>System Details tab</b>	
<b>Computer Model</b>	Model of this computer. Also identifies virtual machines.
<b>Processor</b>	Model, speed, and number of processors for this computer.
<b>Installed Memory</b>	Amount of memory installed on this computer.
<b>Operating System/ Operating System Details</b>	Operating system version on this computer. In the Computers table: <ul style="list-style-type: none"> <li>Operating System shows the basic OS (e.g., Windows 7)</li> <li>Operating System Details includes the full name, the build and service pack level.</li> </ul> On the Computer Details page, the Operating System field shows full details.
<b>Virtualized</b>	Indicates whether the computer is a virtual machine, and if so, its platform. Possible values are: No, Yes (VMware), Yes (Unknown)
<b>AD Details tab</b>	
	Clicking this tab shows any additional computer details available through Active Directory. No information is added if AD integration is not enabled or the AD server is unavailable.
<b>Carbon Black tab</b>	
<b>Sensor Version</b> (Carbon Black Version in table)	The version of the Carbon Black sensor installed on this computer.

Field	Description
<b>Carbon Black Status</b> (in table) <b>Last Status</b> (on Details page)	<p>This field shows the last Carbon Black sensor status for this computer, as reported by the Bit9 Agent to the Bit9 Server. The Bit9 Server checks Carbon Black status every 30 minutes, and so status changes may be out of sync for up to that amount of time.</p> <p>The possible values for Carbon Black Status in the table are:</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• Installed, initializing – sensor is installed but not fully initialized</li> <li>• Installed, running</li> <li>• Installed, not running</li> <li>• Not installed</li> <li>• Stopped</li> </ul> <p>On the Details page, the Last Status field on the Carbon Black tab is similar to Carbon Black Status in the table. However, it does not appear if sensor status is Unknown. Its possible values are:</p> <ul style="list-style-type: none"> <li>• Running</li> <li>• Service not running</li> <li>• Kernel not running</li> <li>• Stopped</li> </ul> <p><b>Notes:</b> In addition to up to a 30-minute gap between sensor installation and Bit9 polling of Carbon Black status, status will continue to report as <i>Not installed</i> until the Carbon Black sensor connects to the Carbon Black server and receives a sensor id. Also, if the Bit9 Agent is offline or uninstalled from a computer, the last Carbon Black sensor status reported by the agent is displayed in the Bit9 Console, even if sensor status changes.</p>
<b>Uptime</b>	Number of minutes and hours that the Carbon Black sensor has been running since it was last started.
<b>Computer Status</b>	The status of this computer as reported by the Carbon Black server.
<b>Registration Time</b>	The date and time the Carbon Black sensor on this computer registered with its server.
<b>Last Checkin</b>	The date and time the Carbon Black sensor on this computer last checked in with its server.
<b>Next Checkin</b>	The date and time of the next scheduled server checkin for the Carbon Black sensor on this computer.
<b>More Information</b>	<p>Connects to the login page of the Carbon Black server configured on the System Configuration page Licensing tab. Logging in takes you to the Sensors page in Carbon Black so you can view additional details about this computer.</p> <p><b>Note:</b> You must have valid login credentials for the Carbon Black server to successfully open the Carbon Black console.</p>
<b>Microsoft SCEP tab</b>	
<b>Deployment State</b>	State of the SCEP agent on this computer. The values are Managed and Unmanaged.
<b>Endpoint Protection</b>	The status of Microsoft Endpoint Protection on this computer. Enabled or Disabled.

Field	Description
<b>Anti-Spyware Protection</b>	The status of Microsoft Anti-Spyware Protection on this computer. Enabled or Disabled.
<b>Anti-Spyware Signature Last Update</b>	The date and time of the last update of Microsoft Anti-Spyware signatures on this computer.
<b>Anti-Virus Protection</b>	The status of Microsoft Anti-Virus Protection on this computer. Enabled or Disabled.
<b>Anti-Virus Signature Last Update</b>	The date and time of the last update of Microsoft Anti-Virus signatures on this computer.
<b>Last Infection</b>	The date and time of the last malware infection detected by SCEP.

Table 17: Computer Details page menus

Menu/Options	Description
<b>Related Views menu</b>	
<b>Recent Events</b>	Opens the Events page and shows recent events (if any) for which this computer was the source.
<b>Health Check Events</b>	Opens the Events page and shows health check events for this computer. Use this information for troubleshooting an agent health check failure with Bit9 Technical Support. If necessary, you can save the resulting events using the <b>Export to CSV</b> button on the events page.
<b>Files on this Computer</b>	Opens the Find Files page to list all tracked files on this computer.
<b>Carbon Black Details</b>	Opens a new browser window or tab showing the login page of the Carbon Black server configured on the System Configuration page Licensing tab. Logging in takes you to the Sensors page in Carbon Black so you can view additional details about this computer. Link appears only if Carbon Black server is configured. <b>Note:</b> You must have valid login credentials for the Carbon Black server to successfully open the Carbon Black console.
<b>Actions menu</b>	
<b>Change Policy</b>	The dropdown menu provides an alternate way to move the computer into another policy. One of the policies available on this menu is Local Approval, which you can use to temporarily place this computer in Local Approval mode. Click the <b>Go</b> button to apply the change. If this computer had its policy assigned automatically, <i>Automatic</i> shows next to the Go button and the menu is not active. You can un-check the Automatic checkbox to remove automatic assignment and then choose a policy from the menu.



Menu/Options	Description
<b>Prioritize Updates/ Remove Prioritization of Updates</b>	<p>Temporarily increases the priority of this computer for receiving upgrades to the agent and configuration lists from the Bit9 Server. A disconnected host can be prioritized while disconnected and the state will be respected when agent comes online next time.</p> <p>Once a computer has been prioritized, this link changes to <i>Remove prioritization of updates</i>. You also can click <i>Remove prioritization...</i> to downgrade a prioritized computer immediately. Once it is up-to-date in all respects, an agent that had Prioritize Updates applied to it automatically returns to normal priority.</p> <p>An agent may also be assigned permanent prioritization status. This is done automatically for computers hosting Trusted Directories. Permanent prioritization also may be assigned through a command on the Advanced/Other Actions menu. The <i>Remove prioritization...</i> command removes both permanent and one-time prioritization.</p>
<b>Request Agent Upgrade/Remove Agent Upgrade Request</b>	<p><i>Request Agent Upgrade</i> schedules this agent for an immediate upgrade. Appears only if the Bit9 Agent is eligible for upgrade.</p> <p><i>Remove Agent Upgrade Request</i> removes the upgrade request and so the agent is not forced to upgrade. This appears only if you have previously scheduled an immediate upgrade request.</p> <p>The options apply only to policies with automatic agent upgrades enabled (See <a href="#">“Advanced Configuration Options”</a> on page 627).</p>
<b>Add files to Snapshot</b>	<p>Adds the list of files on this computer (as stored in the Bit9 Server database) to a <i>snapshot</i> of files. You can use a snapshot to determine how far each of the computers on your Bit9 Server network have drifted from a baseline of known files. Files in a snapshot can have a variety of statuses; if the snapshot contains banned files, they remain banned. See <a href="#">“Managing Snapshots”</a> on page 539 for more detail.</p> <p>There are two options on this menu:</p> <p><b>Choose existing snapshot</b> – Adds the list of files on this computer to the snapshot you choose from a menu.</p> <p><b>Create a new snapshot</b> – Prompts for a new snapshot name and saves the file list of this computer to that snapshot.</p>
<b>Advanced menu</b>	
<b>Convert to Template</b>	<p>Converts the current computer to a Bit9 Security Platform computer <i>template</i>, after which clone computers created from the template’s image (using third-party virtualization/imaging solutions) can be better managed. See <a href="#">Chapter 6, “Managing Virtual Machines,”</a> for more details.</p>
<b>Set Debug Level</b>	<p>Changes the amount of debugging information collected from the agent on this computer. For use in conjunction with Bit9 Support.</p>
<b>Configure Agent Dumps</b>	<p>Changes the amount of information included in file dumps from the agent on this computer. For use with Bit9 Technical Support.</p>
<b>Reset CLI Password</b>	<p>Manually resets the CLI enable code. Allows you to change the enable code after using it with a Bit9 Support representative, so that only your own support users have access to it.</p>



Menu/Options	Description
<b>Disable/Enable Tamper Protection</b>	If agent tamper protection is enabled, clicking Disable Tamper Protection disables it. If protection is disabled, clicking Enable Tamper Protection enables it. Disabling tamper protection is not recommended unless required to solve a particular problem, and the feature should be re-enabled as soon as possible.
<b>Change local state</b>	This menu allows you to locally approve all unapproved files on the computer. You might choose to do this if you have added a large number of known-good files to a computer after initialization.

Menu/Options	Description
<b>Perform Cache Consistency Check</b>	<p>A cache consistency check ensures that the agent on this computer has accurate information about the files actually present. It is necessary only if the agent was not running during a time when files were written to the computer. If the agent requires updating due to the consistency check, any differences are also sent to the server.</p> <p>Changes in the file cache may affect whether or not a file is approved. You can choose one of three levels of cache consistency checking from the menu:</p> <ul style="list-style-type: none"> <li>• <b>Quick Verification:</b> Confirms that each file in the agent's cache exists, verifies that it is still an executable file that should be tracked, and compares the size of each file on disk to the size stored in its cache the last time the file was analyzed. If a file no longer exists, it is removed from the cache. If any of the other checks fail, the file is re-analyzed.</li> <li>• <b>Rescan Known Files:</b> Does everything in the Quick Verification, plus compares the hash of each file on disk to the same file's hash in the agent cache. If the hash does not match, the file is re-analyzed.</li> <li>• <b>Full Scan for New Files:</b> Does everything in the previous two levels, plus rescans the entire disk, looking for files that should be in the agent cache, but are not. Analyzes any file found.</li> </ul> <p>In addition to the menu options, there are three checkboxes that can modify the consistency check:</p> <ul style="list-style-type: none"> <li>• <b>Preserve state of changed files:</b> If the agent does not have a record of a hash in its cache, it will look up the file by name. If that is found, the file state from this record will be used for the current file.</li> <li>• <b>Re-evaluate publishers:</b> Re-examines each file to ensure that its certificate information is accurate and the certificate has not expired or been revoked. Also re-evaluates trusted publisher approvals.</li> <li>• <b>Approve new files:</b> Locally approve new files found during a full scan.</li> </ul> <p><b>Note:</b> This consistency check is a troubleshooting feature that you would normally use in consultation with Bit9 Technical Support. Depending upon the option you choose, a cache consistency check could be a time-consuming operation.</p>
<b>Other Actions submenu</b>	<p>Less frequently needed agent management features, often for use in conjunction with Bit9 Technical Support. The options are:</p> <ul style="list-style-type: none"> <li>• Reboot computer</li> <li>• Upload diagnostic files</li> <li>• Delete diagnostic files on computer</li> <li>• Make local copy of agent cache</li> <li>• Rescan installed applications</li> <li>• Resend all policy rules</li> <li>• Resynchronize all file information</li> <li>• Upload statistics</li> <li>• Run health check</li> <li>• Restore database</li> <li>• Delete database</li> <li>• Restart service</li> <li>• Permanently prioritize updates</li> </ul>

## Moving Computers to Another Policy

Moving a computer into a different policy is a convenient way to change its protection without creating a new policy. From the Computers table, you can select and move computers into different policies. If you have enabled AD-based policy assignment, you can move computers from manual to automatic policy assignment, and vice versa.

### Notes

Changing AD mapping rules *does not* immediately change the policy for an affected computer. The change takes place the next time that computer re-registers with the Bit9 Server. The section [“Assigning Computers to a Policy”](#) on page 102 lists events that trigger agent computer registration.

In addition to the methods described in this section, you can use the Change Policy portlet on the Bit9 Console Home Page.

### To move a computer to another policy:

1. In the console menu, choose **Assets > Computers**. The Computers Page appears:
2. In the Computers table, locate the computer(s) you want to move (using filters or Saved Views, if helpful) and check the associated checkbox for each computer.

Computers

Computers connected: 136 Total computers: 174 Current CL version: 5925348

Saved Views: (The Current View Has Unsaved Changes) (none) Add

Group By: (none) Ascending

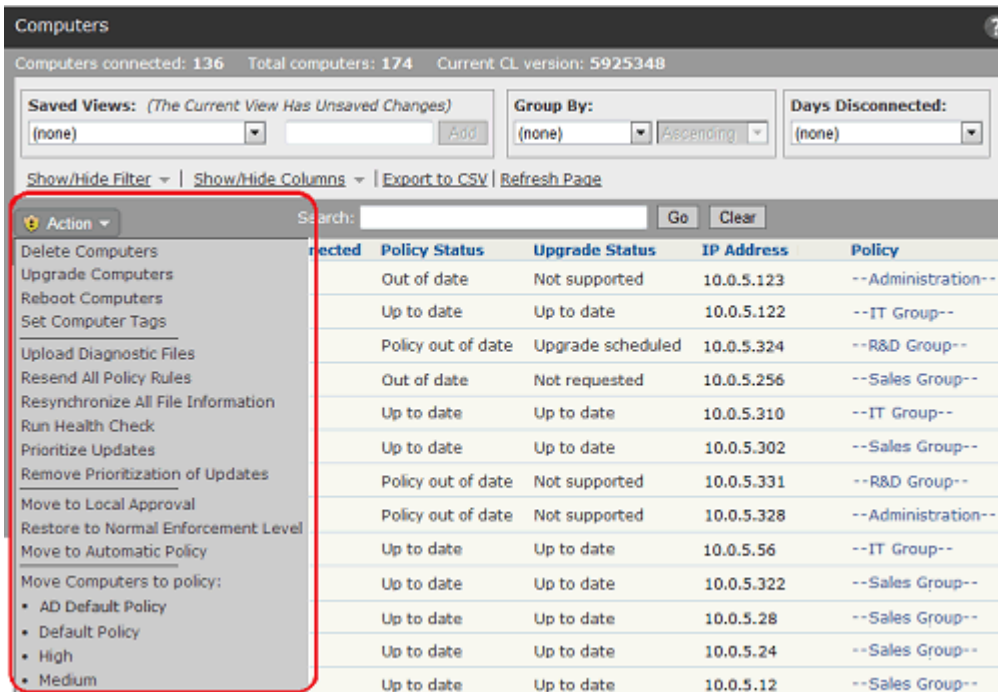
Days Disconnected: (none)

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Action Search: Go Clear

<input type="checkbox"/>	Computer Name	Connected	Policy Status	Upgrade Status	Policy
<input type="checkbox"/>	MYCORP\DESKTOP-3	<span style="color: blue;">●</span>	Out of date	Not supported	-- Administration --
<input checked="" type="checkbox"/>	MYCORP\DESKTOP-7	<span style="color: blue;">●</span>	Up to date	Up to date	-- IT Group --
<input type="checkbox"/>	MYCORP\LAPTOP-5	<span style="color: orange;">●</span>	Policy out of date	Upgrade scheduled	-- R&D Group --

3. Click the **Action** button to see the Action menu.



4. On the Action menu, choose the option that shows the move you want to make. In the confirmation dialog, choose **OK** to reassign the computer to the selected policy. The computer moves to the policy you selected, and if you moved it from Automatic, the policy assignment becomes manual.

### Notes

You also can change a computer's policy by clicking on the computer name in the table and using the Change Policy menu on the Computer Details page.

In addition, Event Rules may be created that will automatically change a computer's policy when certain events occur.

## Restoring Computers from the Default Policy

The Default policy is for computers that report to the Bit9 Server but cannot be associated with any other policy. Causes for this include:

- AD mapping is enabled, the default AD mapping rule (the last rule on the list) maps policies to Default Policy, and an agent does not match any other rule.
- An old installer associated with a deleted policy might be used for the initial Bit9 Agent installation on a computer.
- The last agent in a policy disconnects from the Bit9 Server and then is deleted from the Computers table on the console; because the policy now has no computers, a console operator decides to delete it. The agent later reconnects to the Bit9 Server.

In any of these cases, the computer is automatically moved into the Default Policy. Bit9 recommends that you set the Enforcement Level for the Default policy to the appropriate

protection level for your site. If you set the Default Policy to Visibility Mode, which tracks but does not block file executions, any computers that appear in the Default Policy should be moved as soon as possible to a policy with the settings and Enforcement Level protection you want.

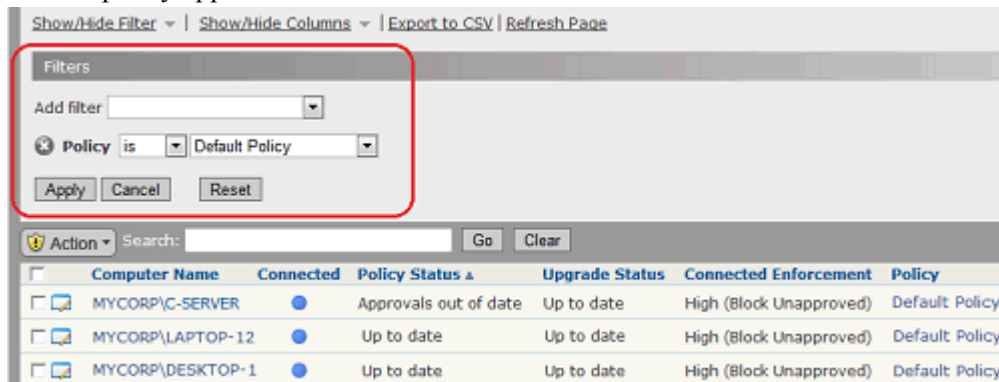
### Notes

- If you do not have any full Suite licenses (Visibility and Control), your only Enforcement Level choices for the Default policy are Visibility and Disabled.
- Because the Default Policy is reserved by the system, you cannot delete it.

The procedure for restoring computers from the Default policy is essentially the same as that for moving computers to another policy, with additional filtering instructions.

#### To move a computer in the Default policy to another policy:

1. In the console menu, choose **Assets > Computers**. The Computers Page appears.
2. If it is not the current choice, choose **(none)** as the Saved View.
3. Click the **Show/Hide Filters** link, and on the Add filter menu, choose **Policy**.
4. In the Policy filter, make sure **is** is the operator, choose **Default Policy** from the rightmost menu, and click the **Apply** button to apply your filter. All computers in the Default policy appear.



5. From the Computers table, check the checkbox(es) for the computer(s) to be moved. You can check multiple computers if you want to move them from the Default policy to the same non-Default policy.
6. On the Action menu, select the policy to which the checked computers are to be moved. If you are using AD-based policy assignment and you are certain this computer matches one of your mapping rules, choose **Move to Automatic Policy**.
7. In the confirmation dialog, click **OK** to reassign the selected computer to the new policy. This temporarily disconnects the Bit9 Server from the agents of any computers checked and causes them to reconnect. When reconnected, the computers are associated with the policy you moved them to.

## Moving a Computer to Local Approval Mode

When computer users need to install new software and Bit9 trusted-approval methods (directory, user/group, publisher and updater) are inappropriate, you can temporarily put the user's computer into Local Approval mode, which is a special policy that permits software installation. Executable files introduced to a computer while it is in Local Approval mode become locally approved on that computer unless already banned. Files already on the computer before you enabled Local Approval mode are not locally approved, although there are other methods to approve them.

You enable Local Approval mode for a computer either by checking the box next to its name on the Computers page and choosing **Move to Local Approval** on the Action menu, or by choosing **Local Approval** on the Change Policy menu on the Computer Details page. See [“Moving Computers to Local Approval Mode”](#) on page 258 for complete instructions.

## Adding Computers

Computers are added to the Computers table when you install the Bit9 Agent on them and they contact the Bit9 Server – there is no special “Add Computer” operation required. If you are using AD-based policy assignment, a new computer is assigned a policy based on the rules you set for mapping AD data for a computer (or its users) to security policies. Otherwise, the computer is assigned the policy specified in the agent installation package chosen for it.

## Deleting Computers

Computers that are no longer in service or that you choose not manage with an agent may be deleted from the Bit9 Server. Before you delete a computer from the Computers table in the Bit9 Console, you first change the computer's Enforcement Level to Disabled and then uninstall the Bit9 Agent. See [“Uninstalling Bit9 Agents”](#) on page 127 for more detail.

If you *do not* uninstall the agent before you delete a computer and that computer remains connected to the same network as your Bit9 Server, the computer will reappear in the computer table as soon as it polls the Bit9 Server. If connected to the network, computers immediately return to the table; if off-line, computers return upon reconnection. Deleted computers that continue to run the agent return to their last recorded policy. If you have deleted the policy applied to the computer by its agent installer, the server moves the computer to the Default Policy.

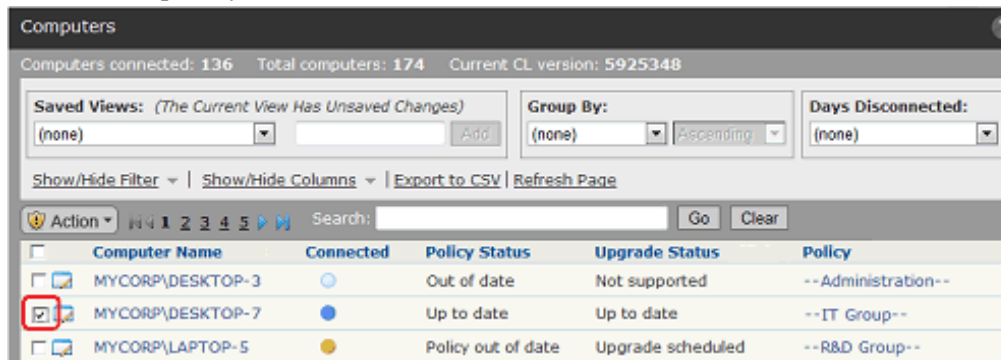
### Note

If a computer running Bit9 Agent cannot connect to the Bit9 Server and you want to remove its agent, contact Bit9 Technical Support.

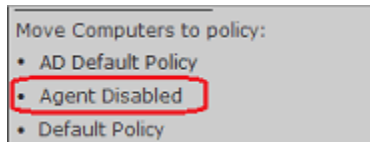
Files on deleted computers remain in the Files on Computers inventory for a short period of time, 24 hours by default. See [“Files on Deleted Computers”](#) on page 605 for an illustration of how these files appear in search results.

**To delete a computer from Bit9 Server:**

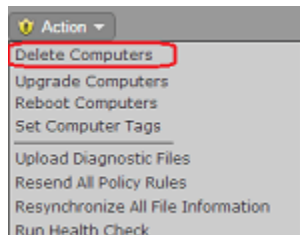
1. In the console menu, choose **Assets > Computers**. The Computers page appears.
2. Find the computer you want to delete and check the checkbox next to its name.



3. In the Action menu, select the Move command for your agent disabled policy from the menu (it is shown as “Agent Disabled” below but you can call it anything you want; it must have an Enforcement Level/Mode of *Disabled*).



4. In the confirmation dialog, click **OK** to trigger the policy change. Watch the description of the computer in the table to see when the change is completed.
5. Once the agent for this computer is in the agent disabled policy and displays an Enforcement Level of *Disabled*, delete the Agent software from the computer itself.
6. On the Computers page, locate the name of the computer whose agent you removed and check the box next to its name.
7. On the Action menu choose **Delete Computers**.

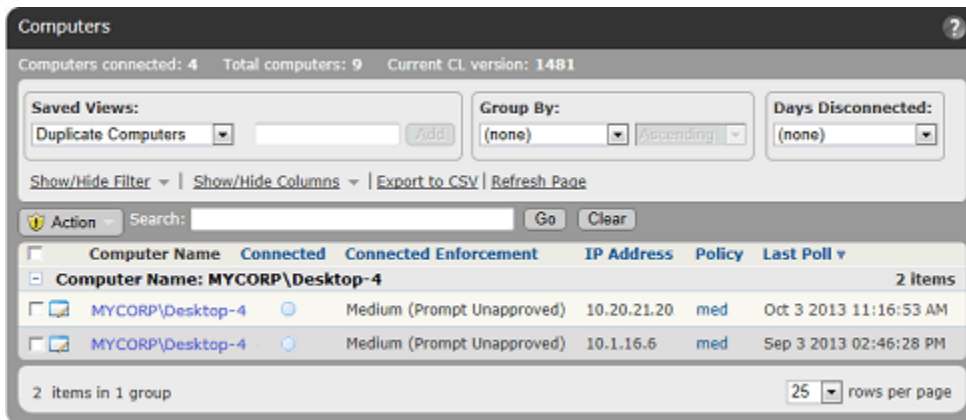


8. On the confirmation dialog, click **OK** to complete the deletion.

**Duplicate Computers**

In some cases, duplicate computer names can appear in the Computers table. This can happen when an agent-managed computer is taken offline, reconfigured or repaired, and then has the agent re-installed without having its previous agent uninstalled and its entry deleted from the table. This presents an asset management problem, one that can become much greater in larger organizations with many computers being reconfigured on a regular basis.

To make it easier to identify and eliminate duplicate computer names, the Computers view includes a Saved View called *Duplicate Computers*. This view lists every agent-managed computer whose name is the same as the name of another agent-managed computer, where neither computer has been deleted in Bit9.



The Duplicate Computers view shows computer grouped by name and includes a *Last Poll* (the date and time when the agent and server last communicated so that you can decide which computer entry represents the currently active agent).

**Note**

You also can add the column *Duplicate* to any Computers table view to identify which computers are duplicates (the value is Yes) and which are not (the value is No).



## Chapter 5

# Creating and Configuring Policies

This chapter explains how to create policies and change their settings, including Enforcement Levels.

### Sections

Topic	Page
<a href="#">Policy and Enforcement Level Overview</a>	150
<a href="#">Creating Policies</a>	151
<a href="#">Policy Settings</a>	156
<a href="#">Editing a Policy</a>	163
<a href="#">Related Views in Policy Details</a>	165
<a href="#">Enforcement Levels</a>	166
<a href="#">Locking Down all Computers</a>	169
<a href="#">Deleting Policies</a>	173

## Policy and Enforcement Level Overview

Each computer running a Bit9 Agent is associated with a Bit9 Security Platform *policy*. A policy creates a common file control definition for all of its computers. Each policy consists of a group of settings and an overall Enforcement Level.

*Policy settings* specify the types of files or operations that Bit9 Agents will control as well as other choices such as how policies are assigned and whether agents on computers in the policy upgrade automatically.

*Enforcement Level* defines how strictly actions defined by the policy settings are controlled, especially for control of file writing and execution. The choices are:

- High (Block Unapproved)
- Medium (Prompt Unapproved)
- Low (Monitor Unapproved)
- None (Visibility)
- None (Disabled)

### Note

High, Medium, and Low Enforcement are available only if you have the full Bit9 Security Platform with both Visibility and Control features. Sites whose licenses are all for Visibility Only operation are limited to Visibility and Agent Disabled modes with no enforcement.

In Visibility mode, you can still choose settings that would block activity if you were operating another Enforcement Level, but these settings do not enforce the block or ban.

## Creating Policies

Policies enable you to organize computers running the Bit9 Agent into groups with common security requirements. For example, you can create policies based on departmental affiliations like sales, marketing, or other organizational relationships. You might also create policies specific to a computer's purpose, such as a special domain controller policy. A single policy may be appropriate if you want a single, company-wide operating standard for all computers, but typically you will create multiple policies.

Policies normally are assigned to computers, not users, although Active Directory data can be used to assign policy by user. Each computer has only one policy at a time, regardless of the number of users currently logged on.

Once a policy is created, you can assign computers to it through a variety of methods, including automatic assignment based on Active Directory group. See [Chapter 4, "Managing Computers,"](#) for more details on policy assignment.

### Important

Policy names can use alphanumeric characters and certain symbols in the ISO-8559-1 set. Characters in the 32-127 range in the ISO-8559-1 set are legal, with the following exceptions: < > : " / \ | ? \* # @

If you enter Unicode characters or reserved symbols in a policy name, the console displays a warning dialog. You must remove the illegal characters from the name before you can save the policy.

Some characters that are allowable in policy names might cause problems when running the agent installer for the policy. For policies that will be applied to Mac computers, avoid parentheses and spaces in the name, or be prepared to "escape" these characters when you run the installer.

**To create a policy:**

1. On the console menu, choose **Rules > Policies**. The Policies page appears:

Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
AD Default	High (Block Unapproved)	High (Block Unapproved)	1	1
Default Policy	High (Block Unapproved)	High (Block Unapproved)	0	0
Domain Controllers	High (Block Unapproved)	High (Block Unapproved)	12	12
Executive Team	High (Block Unapproved)	Medium (Prompt Unapproved)	9	7
Local Approval Policy	Local Approval	Local Approval	0	0
Research Team	Low (Monitor Unapproved)	Low (Monitor Unapproved)	17	15
Sales & Marketing	High (Block Unapproved)	High (Block Unapproved)	21	10
Service Team	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	19	12
Template Policy	None (Visibility)	None (Visibility)	0	0
Uninstall Agent	None (Disabled)	None (Disabled)	0	0

2. On the Policies page, click the **Add Policy** button. The Add Policy page appears (shown below for a Control policy):

**Add Policy**

Policy Name:

Description:

Mode:  Visibility  Control  Disabled

Enforcement Level: Connected: High (Block Unapproved) Disconnected: High (Block Unapproved)

Initial Settings: Template Policy

Automatic Policy Assignment For New Computers:

Options:  Allow Upgrades  Track File Changes  
 Load Agent in Safe Mode  Suppress Logo In Notifier

Total Computers: 0  
 Connected Computers: 0

3. On the Add Policy page, enter a policy name and define the other policy parameters as you choose (see [Table 18](#)) – the parameters you see may vary depending upon other policy settings and configuration choices:

**Table 18:** Policy Definitions: Main Panel

Field	Description
<b>Policy name</b>	<p>Name of the policy.</p> <p>Choose a name that indicates the security level, function, or other common factor for computers or users you want to use this policy.</p> <p><b>Note:</b> Once you create a policy, you cannot change its name, so be sure to choose names that are useful and clear.</p>
<b>Description</b>	<p>Optional information about the policy. This can be any text you choose to enter.</p>
<b>Mode</b>	<p>The mode in which the Bit9 Server interacts with the computers in this policy:</p> <p><b>Visibility</b> specifies file-tracking only. The Bit9 Server tracks file activity and events, but file execution and writing is not effected by policy settings or file bans in place. No Enforcement Level menus appear when you choose Visibility mode.</p> <p>If you have not purchased Control licenses, Visibility is the only mode choice other than Disabled.</p> <p>You might choose to use Visibility when security features have or could interfere with operational functions for computers. For example, you might use Visibility mode for a computer on which you plan to configure a Trusted Directory for files you will allow to be installed on all computers.</p> <p><b>Control</b> activates the Enforcement Level menus, from which you can choose the level of control over execution of Unapproved and Banned files.</p> <p><b>Disabled</b> specifies pass-through mode; the agent neither blocks file activity nor reports it to the server. Executables run as if the agent were not installed. Use this setting for uninstalling the agent.</p> <p>File inventory for computers in Disabled mode will not be kept up to date on the server. Some operations are monitored (but not reported to the server) to avoid gaps in file and process information if the agent is later activated.</p>

Field	Description
<b>Connected Enforcement Level</b>	<p>The protection level for computers in this policy while they are connected to the network (menu only appears in Control mode):</p> <p><b>High (Block Unapproved)</b> is the highest protection level you can set —no Unapproved or Banned files in categories tracked by the Bit9 Security Platform are allowed to run. Blocked file executions are recorded in the event log.</p> <p><b>Medium (Prompt Unapproved)</b> blocks Unapproved executables on agent computers but displays a dialog box that gives users the option to permit or block the file execution. Users cannot permit execution of explicitly Banned files.</p> <p><b>Low (Monitor Unapproved)</b> permits Unapproved executables to run but tracks them. Files allowed to run include running non-executables (such as dlls, com objects and loadable resources), unapproved scripts, and unapproved executables. Events are recorded for the first instance of a permitted file execution and for all blocked executions.</p> <p>At High, Medium or Low Enforcement Levels, determination of which files are blocked also depends on the Advanced Settings within each policy.</p> <p><b>Visibility</b> and <b>Disabled</b>, for which the Enforcement Level is <b>None</b>, are set from the Mode line.</p>
<b>Disconnected Enforcement Level</b>	<p>The protection level for computers in this policy while they are out of communication with the Bit9 Server. If the Connected Enforcement Level is Low (or None) the Disconnected Enforcement Level is identical to the Online, and cannot be modified directly. If the Connected Enforcement Level is High or Medium, you can choose an Disconnected Enforcement Level of High or Medium, and it may differ from the Connected Enforcement Level.</p>
<b>Initial Settings</b>	<p>Existing policy that you would like to use as a template for the new policy. Although not visible when you create a policy, the Device and Advanced Settings (only) of the policy you choose are transferred to the new policy. See <a href="#">“Template Policy”</a> on page 161 for more information.</p>
<b>Automatic Policy Assignment for New Computers</b>	<p>When this box is checked, if AD-based policy assignment is enabled and configured, new computers that used the installer for this policy get their policy according to the AD-mapping rules, regardless of the policy embedded in the installation package used to install their agent. When not checked, the install package determines the policy and AD mappings have no effect. See <a href="#">“Assigning Policy by Active Directory Mapping”</a> on page 103 for more details.</p>
<b>Set automatic policy for existing computers</b>	<p>This checkbox appears only if the <i>Automatic policy assignment for new computers</i> box is checked. When checked, if any computers were manually (non-automatically) assigned to the current policy, they are changed to automatic policy assignment.</p>
<b>Set manual policy for existing computers</b>	<p>This checkbox only appears if the <i>Automatic policy assignment for new computers</i> box is checked. When checked, if any computers were automatically assigned to the policy, they are changed to have this policy manually assigned.</p>

Field	Description
<b>Options: Allow Upgrades</b>	If the Bit9 Server is configured for Automatic Bit9 Agent upgrades, checking this box causes computers in the policy to be notified of and scheduled for Bit9 Agent upgrades. Computers moved into this policy (either manually or by Active Directory mapping) also will be upgraded. See <a href="#">“Advanced Configuration Options”</a> on page 627 and the upgrade sections of <i>Installing the Bit9 Server</i> for more information. For use only during Bit9 Server upgrades.
<b>Options: Track File Changes</b>	<p>When checked (the default) file changes (files added, deleted, or changed) on a computer are tracked and added to the database for this Bit9 Server.</p> <p>You might deselect this option to remediate performance issues, perhaps while waiting to upgrade from SQL Express to a full version of SQL Server, or in a special policy for computers whose file activity you don't want to track.</p> <p><b>Important:</b> If you turn off this feature, Bit9 Server deletes the file inventory information for the agents in this policy after one day. The Files on Computers table, Find Files, and Baseline Drift reports will not provide accurate information about these computers. Also, if you turn this feature on after it has been off, this causes a mandatory re-synchronization of the affected agents to update the file database, and this can have a performance impact.</p>
<b>Load Agent in Safe Mode</b>	<p>Loads the Bit9 Agent in Safe Mode on computers in this policy if the computer is booted in Safe Mode. In this case the agent performs all enforcement activities, even though the system is in Safe Mode. Full protection requires the agent kernel, which loads at boot time, and the agent itself, which runs as a service after boot time.</p> <p><b>Caution:</b> This option should be used only if you have alternative means of recovery, other than using Safe Mode, since the agent can interfere with Safe Mode recovery operations. If you have questions about enabling the agent to run in Safe Mode, contact Bit9 Technical Support.</p>
<b>Suppress Logo in Notifier</b>	When any Bit9 rule displays a notifier on an agent in this policy, do not show a logo, even if the rule's notifier definition includes a logo.
<b>Total/Connected Computers</b>	<p><b>Total Computers</b> - The total number of computers managed by this policy on the Bit9 Server. Computers by platform is shown in parentheses.</p> <p><b>Connected Computers</b> - The number of computers managed by this policy currently connected to the Bit9 Server. Computers by platform is shown in parentheses.</p>

4. After you have provided the policy configuration parameters on this page, click the **Save** button. The new policy appears in the table on the Policies page.
5. To modify the Device Settings or Advanced Settings for this policy, click the View Details (pencil) button next to the new policy name, make your modifications, and click **Save**. See [“To edit a policy:”](#) on page 163 for detailed instructions on editing these settings. Note that Device and Advanced Settings do not appear on the Add Policy page – you must save the policy first to see them.

### Notes

For more information about the Device Settings and other device monitoring and control features in the Bit9 Security Platform, see [Chapter 11, “Managing Devices.”](#)

For information about customizing the notifier displayed on a client computer when policy and ban settings are enforced, see [Chapter 17, “Block Notifiers and Approval Requests.”](#)

## Policy Settings

The Enforcement Level for a policy sets the overall security level and determines whether the policy is configured to block or permit execution of Unapproved files. More specific behavior is controlled by detailed policy settings, which are divided into Device Settings and Advanced Settings. [Chapter 11, “Managing Devices,”](#) describes Device Settings.

### Important

Visibility mode allows you to activate settings that block files, but these settings have no effect while a computer is in Visibility mode. To enable file blocking and other control features, a policy must be in Control mode. You still might activate these settings in Visibility mode for information purposes, or if you plan a change to Control mode in the future.

## Advanced Settings

When active, advanced settings block specified file activities and enforce other rules.

Name	Status	Notifiers
Block unanalyzed scripts and executables	Active	<default>: Block unanalyzed scripts and executables
Block unapproved scripts	Active	<default>: Block unapproved scripts
Block unapproved executables	Active	<default>: Block unapproved executables
Block banned file names	Active	<default>: Block banned file names
Block banned file hashes	Active	<default>: Block banned file hashes
Block executables run from a network drive	Off	<default>: Block executables run from a network drive
Block files with banned publishers or certificates	Active	<default>: Block files with banned publishers or certificates
Enforce memory rules	Active	<default>: Enforce memory rules
Enforce registry rules	Active	<default>: Enforce registry rules
Enforce custom (file and path) rules	Active	<default>: Enforce custom (file and path) rules
Enforce tamper protection	Active	<default>: Enforce tamper protection
Terminate processes with banned images	Report Only	<default>: Terminate processes with banned images

Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High

Because any file or activity is usually affected by more than one rule, turning a setting off can have varying results. There are three possible options for advanced settings:



**Table 19:** Policy Advanced Setting Options

Setting Options	Description
<b>Active</b>	Setting is enabled. Files are blocked or permitted according to the specified Enforcement Level.
<b>Off</b>	Setting is disabled and not enforced under any Enforcement Level. Files matching the setting continue to be tracked but are not blocked.
<b>Report Only</b>	A test state that permits actions that would have been blocked if the setting were active and records a <i>would-have-blocked</i> event in the Events table. You can use it to verify that settings and Enforcement Level in a policy work as intended, without actually blocking any files.

Turning off one setting that *blocks* an action or file does not necessarily mean the action or file is *permitted*; similarly, turning off one setting that *permits* an action does not necessarily mean that the action or file is *blocked*. The Events page might provide an explanation of why a file you expected to be permitted was blocked.

[Table 20](#) shows the Advanced Settings and the effect of setting them to “Active” or “Off”. Some settings cannot be turned off, but are included so you can change or disable the *Notifier* that appears when they block a file execution.

#### Notes

- There are different settings for “executables” and “scripts”. The Bit9 Security Platform determines whether a file is executable based on content, not file extension alone, while scripts are identified by file extension. After examining a file, the Bit9 Agent applies the appropriate policy setting based on the file’s content. See [Chapter 13, “Script Rules,”](#) for information about how scripts are defined in the Bit9 Security Platform.
- Each setting has a Notifiers menu from which you can choose the notifier that appears on an agent computer when that setting in this policy blocks an action. See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for information about choosing and defining notifiers.
- For more about banning software, see [“Approving and Banning Software”](#) on page 223. For more information about creating custom rules for special treatment of files at certain paths, see [Chapter 12, “Custom Software Rules.”](#)

**Table 20:** Advanced Setting Behavior

Setting	Active	Off
<b>Block unanalyzed scripts and executables</b>	<p>Tracks executables (for example, .exe, .dll, and .com) and script files (for example, .bat, .vbs) that have not yet been analyzed and blocks them for systems in High, Medium, and Low Enforcement Levels, and in Local Approval mode.</p> <p>Scripts and executables are reported as unanalyzed if a user or process tries to execute them and the Bit9 Security Platform cannot finish its run-time checks of file state in the expected time. This usually happens when the root certificate for a file is out of date or otherwise not verifiable.</p>	Permits unanalyzed executables and script files to execute if no other settings prevent execution. Not recommended.
<b>Block unapproved scripts</b>	<p>Tracks script files (for example, .bat, .vbs) that have an unapproved status and blocks them according to Enforcement Level:</p> <ul style="list-style-type: none"> <li>• High Enforcement Level blocks unapproved scripts.</li> <li>• Medium Enforcement Level blocks unapproved scripts but presents a dialog that identifies the file and gives users the option to run it.</li> <li>• Low Enforcement Level permits files to execute; records an event the first time the executable runs.</li> </ul> <p><b>Note:</b> <a href="#">Table 53</a> in <a href="#">Chapter 13</a>, “<a href="#">Script Rules</a>,” shows the file types considered scripts by the Bit9 Security Platform.</p>	Permits script files not explicitly banned to execute if no other settings prevent execution.
<b>Block unapproved executables</b>	<p>Tracks executable files, for example, .exe, .dll, and .com, that have an unapproved status and blocks or permits them according to Enforcement Level:</p> <ul style="list-style-type: none"> <li>• High Enforcement Level blocks all unapproved executables.</li> <li>• Medium Enforcement Level blocks unapproved executables but presents a dialog that identifies the file and gives users the option to run it.</li> <li>• Low Enforcement Level permits files to execute; records an event the first time the file runs.</li> </ul>	Permits unapproved files not explicitly banned to execute if no other settings prevent execution.
<b>Block banned file names</b>	Blocks execution of files banned by file name on computers in Control mode.	Cannot be disabled on the policy page, but individual bans can be configured to be policy-specific.

Setting	Active	Off
<b>Block banned file hashes</b>	Blocks all banned hashes on computers in Control mode.	Disables the Banned Hashes setting and permits banned hashes to execute if no other settings prevent it.
<b>Block executables run from a network drive</b>	Blocks execution of files (including Approved files) run over the network on computers in Control mode. <b>Platform Note:</b> This setting is effective for Windows agents only.	Permits network executable files not unapproved or explicitly banned to execute if no other settings prevent it.
<b>Block files with banned publishers or certificates</b>	Blocks execution of files with banned publishers (or certificates) in Control mode.	Permits files with banned publishers/certificates to execute if no other settings prevent it.
<b>Enforce memory rules</b>	Apply all enabled memory access, control, and reporting rules. <b>Platform Note:</b> This setting is effective for Windows agents only.	Cannot be disabled on the policy page, but individual rules can be configured to be policy-specific.
<b>Enforce registry rules</b>	Apply all enabled registry access and reporting rules to this policy. <b>Platform Note:</b> This setting is effective for Windows agents only.	Cannot be disabled on the policy page, but individual rules can be configured to be policy-specific.
<b>Enforce custom (file and path) rules</b>	Apply all enabled custom rules (special treatment of files at defined paths) to this policy. You configure custom rules by choosing Software Rules in the console menu and clicking on the Custom tab.	Cannot be disabled on the policy page, but individual rules can be configured to be policy-specific.
<b>Enforce tamper protection</b>	Apply rules to prevent tampering with a Bit9 Agent.	Cannot be disabled for a policy. Contact Bit9 Technical Support for assistance if you need to turn off tamper protection for a specific computer.
<b>Terminate processes with banned images</b>	When a file is banned, terminate currently running processes that match the file.	Permits a file that is banned while already running to continue running.

Setting	Active	Off
<b>Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High</b>	When checked, causes certain Unapproved files to be locally approved when the policy Enforcement Level changes from Low (or None) to Medium or High. This only applies to files that first appeared on the computer as Unapproved when the computer was in a Low (or None) Enforcement Level policy. These files have Local State Details of "Unapproved".  See <a href="#">"Locally Approving Files"</a> on page 252 for more on local approval methods.	When not checked, Enforcement Level changes do not affect local file state in this policy.

## Template Policy and Default Policy

### Default Policy

The Bit9 Security Platform includes a built-in policy named Default Policy. This is the policy to which computers are assigned in the following situations:

- If you are using AD Mapping to assign policies, the Bit9 Security Platform is initially configured to assign a computer that does not match any other mapping rules to the Default Policy. You can, however, change the policy to which unmatched computers are assigned, and it is generally advisable to create a separate "AD Default" policy for this purpose. See ["Assigning Policy by Active Directory Mapping"](#) on page 103 for more information.
- When computers in a non-existent (deleted) policy report to the Bit9 Server, they are automatically moved into the Default Policy and subject to enforcement based on the default settings. See ["Restoring Computers from the Default Policy"](#) on page 144 for information about how you might deal with this situation.

If you are licensed for Control features, you can set the Default Policy Enforcement Level to High (Block Unapproved) to make sure that if a computer is switched to the Default Policy, neither Banned nor Unapproved files are allowed to run. If you are less concerned about Unapproved files but still do not want to allow them to execute without user interaction, you can set the Enforcement Level to Medium. You also can edit any of the other settings for the Default Policy.

#### Note

Computers can be assigned to the Default Policy unexpectedly. Because of this, the initial policy setting for "Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High" is *off* (un-checked). Otherwise an unexpected transition to the Default Policy could locally approve many files without you wanting that to happen. See ["Automatic Local Approval on Enforcement Level Change"](#) on page 253 for more details about this setting.

## Template Policy

The built-in Template Policy is intended as a “template” for creating other policies. By default, the initial Device and Advanced settings of the first policy you create are based on the settings of this Template Policy, although you can base the initial settings on any other existing policy, including the Default Policy.

### Note

Policies inherit only the *Device Settings* and *Advanced Settings* from their template policy. Settings on the top panel of the Add/Edit Policy page, including Enforcement Level, are not inherited. Device Settings and Advanced Settings appear on the Edit Policy page once you save a new policy.

You can edit the Template Policy to include the Device and Advanced settings you expect to want most of the time, simplifying policy creation. Once you create a policy, there is no ongoing linkage to its template policy, so you can change any setting in the new policy.

One important part of policy configuration is assigning notifiers to each setting in the policy that could block an action. Each policy setting has a notifier assigned to it (or no notifier, if you choose), and the messages can differ depending on the setting that caused the block. If you want to change the messages from their defaults, it is best to alter the Template Policy *before* you create other policies. See [“Customizing and Creating Notifiers”](#) on page 450 for more information.

A key difference between the Template Policy and the Default Policy is the Advanced Setting called "Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High". Activating this setting usually makes sense for a newly created policy, so it is activated by default (and not shown) for the Template Policy.

The Template Policy has the following special characteristics:

- it appears only on the Policies page and its own Edit page
- it cannot be assigned to any computer
- no AD mapping rules can be created that point to the Template Policy
- there is no agent installation package corresponding to the Template Policy
- like the Default Policy, the Template Policy cannot be deleted
- the setting "Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High" is not shown but is automatically activated

### Important

When you create a new policy, be sure to verify or, if needed, change the setting values you inherited from the existing policy you based it on.

## Resetting a Policy to Template Policy Settings

The Edit Policy page for each policy includes a **Reset Policy** button immediately below the Device Settings table.

Name	Status	Notifiers	
Block writes to unapproved removable devices	Off	<default>: Block writes to unapproved removab	Add Edit
Block writes to banned removable devices	Active	<default>: Block writes to banned removable d	Add Edit
Report reads from unapproved removable devices	Off	<none>	
Report reads from banned removable devices	Off	<none>	
Block executions from unapproved removable devices	Off	<default>: Block executions from unapproved r	Add Edit
Block executions from banned removable devices	Active	<default>: Block executions from banned remo	Add Edit

Save Cancel **Reset Policy** Show Advanced Settings

When you press this button and choose **OK** on the confirmation dialog, the Device and Advanced settings are reset to the *current* settings of the Template Policy.

### Important

Once you click **OK** in the reset dialog box, the policy settings are reset without requiring that you click **Save**. To prevent the reset, you must cancel in the *confirmation dialog box*. You cannot prevent the changes by clicking **Cancel** on the Edit Policy page.

## Tamper-Protection Setting

A tamper-protection setting blocks attempts to write to the Bit9 application directory or change Bit9 Agent files on client computers. Tamper-protection cannot be disabled on a per-policy basis, although you can use the Advanced menu on the Computer Details page to disable it for an individual system – consult with Bit9 Technical Support before changing this setting.

Computer users are not permitted to uninstall the Agent unless the computer is in Agent Disabled mode.

### Note

You can specify your own directory-protection policies. See [Chapter 12, “Custom Software Rules.”](#)

For more information about removing Bit9 Agent from a computer, see [“Uninstalling Bit9 Agents”](#) on page 127.

## Editing a Policy

You can edit the basic definitions of a policy, including its description, and Enforcement Level, in the upper panel of the Edit Policy page. The Policy *name* cannot be changed.

For most Device and Advanced Settings, you can:

- turn them on or off
- place them in report-only state, in which they report what they would have done if they had been activated
- choose a different (or no) *notifier*, which is the dialog box that is displayed when an action is blocked as a result of an active policy setting; this is covered in [Chapter 17](#), “Block Notifiers and Approval Requests.”

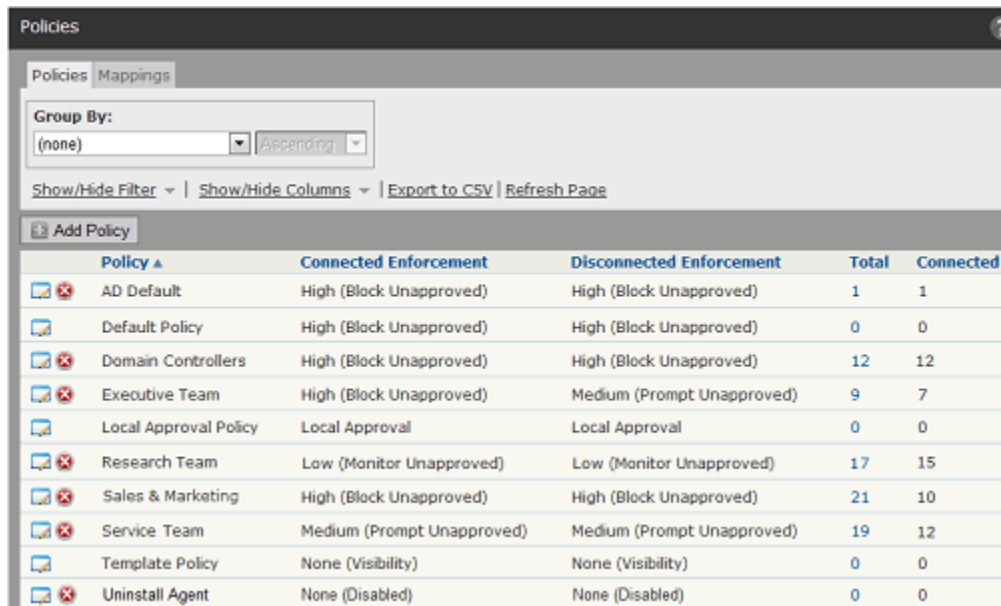
Certain settings have fewer choices or choices other than those on this list.

### Notes

Although you can deactivate policy settings, you cannot create or delete them. The setting name (e.g., *Block unapproved scripts*), which is standard for all policies, cannot be changed.

### To edit a policy:

1. On the console menu, choose **Rules > Policies**. The Policies page appears:



Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
AD Default	High (Block Unapproved)	High (Block Unapproved)	1	1
Default Policy	High (Block Unapproved)	High (Block Unapproved)	0	0
Domain Controllers	High (Block Unapproved)	High (Block Unapproved)	12	12
Executive Team	High (Block Unapproved)	Medium (Prompt Unapproved)	9	7
Local Approval Policy	Local Approval	Local Approval	0	0
Research Team	Low (Monitor Unapproved)	Low (Monitor Unapproved)	17	15
Sales & Marketing	High (Block Unapproved)	High (Block Unapproved)	21	10
Service Team	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	19	12
Template Policy	None (Visibility)	None (Visibility)	0	0
Uninstall Agent	None (Disabled)	None (Disabled)	0	0

2. On the Policies page, click the View Details (file and pencil) button next to the name of the policy you want to edit. The Edit Policy page appears:



**Edit Policy Research Team**

**Policy Name:** Research Team  
**Description:**

**Mode:**  Visibility  Control  Disabled

**Enforcement Level:** Connected: Medium (Prompt Unapproved) | Disconnected: Medium (Prompt Unapproved)

**Automatic Policy Assignment For New Computers:**

**Set Automatic Policy For Existing Computers:**  (Affects 9 computer(s) in this policy which are currently set to manual.)

**Options:**  Allow Upgrades  Track File Changes  
 Load Agent in Safe Mode  Suppress Logo In Notifier

**Total Computers:** 59 ( 59 Windows )  
**Connected Computers:** 52 ( 52 Windows )

---

**Device Control Settings for Research Team**

Name	Status	Notifiers	
Block writes to unapproved removable devices	Off	<default>: Block writes to unap	Add Edit
Block writes to banned removable devices	Active	<default>: Block writes to banr	Add Edit
Report reads from unapproved removable devices	Off	<none>	
Report reads from banned removable devices	Off	<none>	
Block executions from unapproved removable devices	Off	Block executions from unappr	Add Edit
Block executions from banned removable devices	Active	Block executions from banned	Add Edit

3. Edit any of the details in the main panel by checking or un-checking the appropriate box, entering text, choosing a different mode and/or choosing a different Enforcement Level. Visible parameters may vary depending upon other policy settings and configuration choices. See [Table 18, “Policy Definitions: Main Panel,”](#) on page 153 for detail on these settings.
4. From the Edit Policy page, click the **Show Advanced Settings** button to see the rest of the settings associated with this policy.

**Advanced Settings for Special Privilege**

Name	Status	Notifiers	
Block unanalyzed scripts and executables	Active	<default>: Block unanalyzed scripts and execut	Add Edit
Block unapproved scripts	Active	<default>: Block unapproved scripts	Add Edit
Block unapproved executables	Active	<default>: Block unapproved executables	Add Edit
Block banned file names	Active	<default>: Block banned file names	Add Edit
Block banned file hashes	Active	<default>: Block banned file hashes	Add Edit
Block executables run from a network drive	Off	<default>: Block executables run from a networl	Add Edit
Block files with banned publishers or certificates	Active	<default>: Block files with banned publishers or	Add Edit
Enforce memory rules	Active	<default>: Enforce memory rules	Add Edit
Enforce registry rules	Active	<default>: Enforce registry rules	Add Edit
Enforce custom (file and path) rules	Active	<default>: Enforce custom (file and path) rules	Add Edit
Enforce tamper protection	Active	<default>: Enforce tamper protection	Add Edit
Terminate processes with banned images	Report Only	<default>: Terminate processes with banned im	Add Edit

Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High



5. In the Device Control Settings table, use the dropdown menu to select one of the following states for any setting you want to change: **Off**, **Active**, and **Report Only** (*Active* is not a choice for the Read settings). See [Table 43, “Device Control Setting Behavior,”](#) on page 318 for information about these settings.  
**Platform Note:** Visibility and control features for devices are effective for Windows computers only.
6. In the Advanced Settings table, use the dropdown menu to select one of the following states for settings you want to change: **Active** (on), **Report Only** (on, but not enforced), or **Off**. See [Table 20, “Advanced Setting Behavior,”](#) on page 158 for information about these settings.  
**Note:** Some Advanced settings cannot be changed. Fixed settings show their value in a grayed-out menu box.
7. If you want to change the setting for *Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High*, check or un-check the box.
8. If you want to customize the notifier shown by a Device or Advanced setting when it blocks actions on an agent computer, you can choose a different notifier from the Notifiers menu next to the setting, **Edit** the notifier (which affects all places in which this notifier is used), or **Add** and define a new notifier. See [“Customizing and Creating Notifiers”](#) on page 450 for more information.
9. When you have finished changing policy settings, click **Save**. Your changes are saved and the Policies table is re-displayed.

## Related Views in Policy Details

The Edit Policy page has a Related Views menu with links that provide information about files and file rules related to the policy:

- *All files on computers in this policy* opens a Find Files page with all instances of tracked files on the computers assigned to the policy.
- *Unapproved files on computers in this policy* opens a Find Files page with all file instances with a *Local State* of Unapproved on the computers assigned to this policy. This helps show how the policy settings affect the files actually on these computers. You can add another filter to the results to show only files with *Local State Details* of Unapproved – these would be approved by an Enforcement Level change from Low to either Medium or High if the automatic approval box is checked for this policy.
- *File bans and approvals that apply to this policy* opens a filtered view of the Software Rules/Files tab, showing file bans and file approvals that either apply to all policies or specify that they apply to this policy. This may be useful in deciding whether to change the Enforcement Level or other settings in this policy.
- *Computers manually assigned to this policy* opens a filtered view of the Computers page, showing computers that have been manually assigned to the policy (i.e., were not assigned by AD mapping).

## Enforcement Levels

Enforcement Level is the protection level applied to computers running the Bit9 Agent, specified on a per-policy basis. Enforcement Levels, which vary in restrictiveness, affect how file actions are controlled for policy settings. File-blocking and other control functions in the Bit9 Security Platform depend on both the Enforcement Level and on more specific policy settings in effect, including policy-specific bans.

In Control mode, you choose High (Block Unapproved), Low (Monitor Unapproved), or Medium (Prompt Unapproved) Enforcement Level from a menu. The other modes, None (Visibility) and None (Disabled), automatically designate the Enforcement Level as None.

**Table 21:** Enforcement Levels

Enforcement Level	Use when:
<b>High (Block Unapproved)</b>	<p>For the highest protection level, and when it is practical to pre-approve the applications you need and want to run on computers in the policy, use High enforcement.</p> <p>High enforcement permits only explicitly approved files to run. Computers on which the application configuration seldom changes – servers or single-purpose systems, for example – are good candidates for High enforcement. For computers with more dynamic application configurations, High enforcement might be usable <i>if</i> you also pre-approve files via trusted directories, trusted users, approved publishers, enabled updaters, or reputation approvals.</p> <p>Except for files already identified and banned on the Bit9 Server, all files that exist on computers before you install the Bit9 Agent are locally approved and permitted to run on that computer under High enforcement.</p> <p>High enforcement is available to policies in Control mode.</p>
<b>Medium (Prompt Unapproved)</b>	<p>To operate in a condition that prevents unchallenged execution of unapproved files but does not completely block them, use Medium enforcement.</p> <p>Medium enforcement blocks all Unapproved files from executing but displays a dialog on client computers that lets the user decide whether to run the file. If the user allows the file to run, it is locally approved on that computer and always permitted to run. If the Unapproved file is run remotely from a network share or removable device, it is temporarily approved to run (the approval remains for three days).</p> <p><b>Platform Note:</b> Some removable or network drives are not recognized by the Bit9 Security Platform, especially on non-Windows systems. Files run from these drives are treated like local files.</p> <p>Explicitly banned files cannot run under Medium enforcement.</p> <p>Medium enforcement is available to policies in Control mode.</p>

Enforcement Level	Use when:
<b>Low (Monitor Unapproved)</b>	<p>When you are not concerned about unknown files and only need to block files that you have specifically banned, use Low enforcement.</p> <p>Low enforcement blocks banned files while allowing users to install software that are Approved or Unapproved (neither banned nor approved). Although Unapproved files are permitted to execute, you can monitor them and respond with emergency lockdown if necessary.</p> <p>Low enforcement is available to policies in Control mode.</p>
<b>None (Visibility)</b>	<p>To track file activity without blocking it, set the Enforcement Level to None (Visibility).</p> <p>Visibility mode tracks executable file activity on your computers through Bit9's reporting and asset management features (drift reports, event reports, file inventory, etc.), but enforces no rules. It can be a first step on the way to implementing a more controlled environment.</p> <p>Click Visibility in the Mode line to choose this level.</p>
<b>None (Disabled)</b>	<p>To stop all enforcement and tracking activities, choose None (Disabled) mode. You might do this if:</p> <ul style="list-style-type: none"> <li>• You are instructed to disable an agent by Bit9 support staff so that you can debug a system fault.</li> <li>• You plan to remove the Bit9 Agent from a computer; a computer <i>must be</i> in None (Disabled) mode before the agent is deleted and the computer is removed from the Bit9 Server.</li> </ul> <p>If you disable the agent for a computer, that computer's file database is deleted from the agent computer but remains on the server for one day. Computers in Agent Disabled mode re-initialize their files as soon as you move them to a policy at another Enforcement Level.</p> <p><b>Note:</b> An agent in None (Disabled) mode continues to monitor (but not report to the server) certain operations to avoid gaps in file and process information if the agent is later brought back into an active mode. This normally requires a very minimal amount of resources on the agent computer, although if an extremely large number of writes are performed, the impact may be noticeable.</p> <p>Click Disabled in the Mode line to choose this level.</p>

## How Enforcement Levels Affect Policy Setting Enforcement

Enforcement Levels interact with policy settings and other rules to control the conditions under which different types of files actions are allowed. [Table 22](#) shows how file activity is affected for different combinations of Enforcement Level and:

- Advanced Policy Settings and network-wide file bans that are *Active*
- Device Control Settings that are set to *Active*

**Table 22:** Effects of Active Policy Settings by Enforcement Level

Active Policy Settings	Enforcement Levels				
	None (Disabled)	None (Visibility)	Low (Monitor Approved)	Medium (Prompt Unapproved)	High (Block Unapproved)
Block unanalyzed scripts & executables	off	allow	block	block	block
Block unapproved scripts	off	allow	allow	prompt	block
Block unapproved executables	off	allow	allow	prompt	block
Block banned file names (cannot be disabled)	off	allow & report	block	block	block
Block banned file hashes	off	allow & report	block	block	block
Enforce memory rules (cannot be disabled)**	off	non-blocking action & report	block (if specified)	block (if specified)	block (if specified)
Enforce registry rules (cannot be disabled)**	off	non-blocking action & report	block (if specified)	block (if specified)	block (if specified)
Enforce custom (file and path) rules (cannot be disabled)**	off	non-blocking action & report	block (if specified)	block (if specified)	block (if specified)
Enforce tamper protection (cannot be disabled)	basic	full	full	full	full
Terminate processes with banned images	off	continue & report	terminate	terminate	terminate
Block executables run from a network drive *	off	allow & report	block	block	block
Block writes to unapproved removable devices *	off	allow & report	block	block	block
Block files with banned publishers or certificates	off	allow & report	block	block	block
Block writes to unapproved removable devices *	off	allow & report	block	block	block
Block writes to banned removable devices *	off	allow & report	block	block	block
Report reads from unapproved removable devices*	off	allow & report	allow & report	allow & report	allow & report
Report reads from banned removable devices*	off	allow & report	allow & report	allow & report	allow & report
Block execution from unapproved removable devices *	off	allow & report	block	block	block
Block execution from banned removable devices *	off	allow & report	block	block	block

\* Device and Network Drive rules apply to Window computers only.  
 \*\* The possible actions for memory, registry and custom rules include many non-blocking options.

**Notes**

- When an attempt to execute an Unapproved file generates a dialog in Medium Enforcement, either choice (block or allow) is recorded as an event. Also, with Enforcement Level set to Low, execution of an Unapproved file generates an event.
- The Related Views menu on the Edit Policy page includes a link *Unapproved files on computers in this policy*. Since Enforcement Level affects how unapproved files are handled, this link can help you decide how to set Enforcement Level, or whether to leave a given computer in its current policy.

**Special Enforcement Level for Local Approval**

The Bit Security Platform sets a special Enforcement Level for computers in local approval. This Enforcement Level is reserved for system use, and cannot be chosen directly. It enables local approval of software, especially for computers otherwise under High Enforcement

**Changing Policy Enforcement Levels**

If you want to change the level of rule enforcement for a group of computers, you might move them to a different policy. Moving computers is described in [“Moving Computers to Another Policy”](#) on page 143.

Another alternative is to raise or lower the Enforcement Level applied to the *current* policy, using one of the following methods:

- If you are already in Control mode and want to stay there, you can switch between control Enforcement Levels by editing a policy’s Connected Enforcement Level and Disconnected Enforcement Level menus. For example, to increase protection you can switch policies under Low (Monitor Unapproved) Enforcement Level or Medium (Prompt Unapproved) Enforcement Level to High (Block Unapproved) Enforcement Level.
- If you are already in Control mode and want to eliminate control, you can switch to Visibility mode, which changes the Enforcement Level to None (Visibility).
- If you are in Visibility mode, you can switch to Control mode and choose a new Enforcement Level from the menus.

**Important**

Disabling and re-enabling a large number of agents in one operation is not recommended. Switching *to* Agent Disabled mode eliminates enforcement, reporting, and tracking provided by the Bit9 Agent. Switching back *from* Agent Disabled can have significant performance impact, based upon the number of agents in a policy. Each agent switching *out of* Agent Disabled mode reinitializes, going through the same process as a newly installed agent.

**To change Enforcement Level for a policy in Control mode:**

1. On the console menu, choose **Rules > Policies**. The Policies page appears:

Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
AD Default	High (Block Unapproved)	High (Block Unapproved)	1	1
Default Policy	High (Block Unapproved)	High (Block Unapproved)	0	0
Domain Controllers	High (Block Unapproved)	High (Block Unapproved)	12	12
Executive Team	High (Block Unapproved)	Medium (Prompt Unapproved)	9	7
Local Approval Policy	Local Approval	Local Approval	0	0
Research Team	Low (Monitor Unapproved)	Low (Monitor Unapproved)	17	15
Sales & Marketing	High (Block Unapproved)	High (Block Unapproved)	21	10
Service Team	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	19	12
Template Policy	None (Visibility)	None (Visibility)	0	0
Uninstall Agent	None (Disabled)	None (Disabled)	0	0

2. On the Policies page, click the View Details (file and pencil) button next to the policy name you want to edit. The Edit Policy page appears:

**Edit Policy Research Team**

Policy Name: Research Team  
 Description: [Text Area]

Mode:  Visibility  Control  Disabled

Enforcement Level: Connected: Medium (Prompt Unapproved) | Disconnected: Medium (Prompt Unapproved)

Automatic Policy Assignment For New Computers:

Set Automatic Policy For Existing Computers:  (Affects 9 computer(s) in this policy which are currently set to manual.)

Options:  Allow Upgrades  Track File Changes  
 Load Agent in Safe Mode  Suppress Logo In Notifier

Total Computers: 59 ( 59 Windows )  
 Connected Computers: 52 ( 52 Windows )

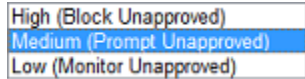
**Device Control Settings for Research Team**

Name	Status	Notifiers	
Block writes to unapproved removable devices	Off	<default>: Block writes to unap	Add Edit
Block writes to banned removable devices	Active	<default>: Block writes to banr	Add Edit
Report reads from unapproved removable devices	Off	<none>	
Report reads from banned removable devices	Off	<none>	
Block executions from unapproved removable devices	Off	Block executions from unappr	Add Edit
Block executions from banned removable devices	Active	Block executions from banned	Add Edit

Buttons: Save, Cancel, Reset Policy, Show Advanced Settings

3. If you want to switch modes, click the button next to the mode you want.
4. To change Enforcement Level within Control mode, select a Connected Enforcement Level from the dropdown menu:





5. If you chose High or Medium for *Connected Enforcement Level*, you can choose a different *Disconnected Enforcement Level* from its dropdown menu.
6. Make any other needed changes to the policy. See “[Policy Settings](#)” on page 156 for details of policy settings.
7. To save the changes, click the **Save** button at the bottom of the page.

## Locking Down all Computers

The Bit9 Console Home page includes an emergency Lockdown button that changes the Enforcement Level of all Bit9-Security-Platform-managed computers to High. During an emergency lockdown, the following is true for active agents whose policies do not have any enforcement settings disabled:

- Banned files are blocked.
- All Unapproved files that appear *after* the emergency lockdown are blocked.
- All existing Unapproved files that *remain* Unapproved are blocked.
- Certain files become locally approved, as described below, and can be executed.
- Computers that were offline when emergency lockdown was initiated are locked down upon reconnection to the Bit9 Server if the lockdown remains in effect.
- Lockdown affects all active agents, including those in Visibility Only mode. It does not affect computers whose agents are disabled.

In some cases, locking down a computer causes some Unapproved files to become locally approved. In the Advanced Settings panel of the Edit Policy page, there is a checkbox labeled “[Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High](#)”. This affects computers whose Enforcement Levels are Low or None when they are moved to Enforcement Levels of High or Medium:

- If the box is checked, existing Unapproved files that first appeared on a computer when it was in Low (or None) Enforcement Level are locally approved upon lockdown.
- If the box is not checked, Unapproved files on computers in that policy remain Unapproved after lockdown and are not allowed to run.

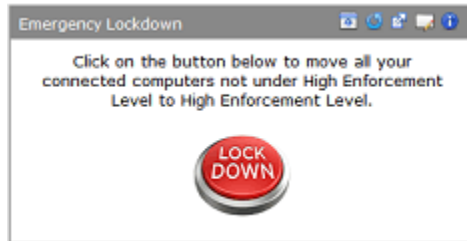
Bit9 Console users with the default ReadOnly privileges do not have access to Emergency Lockdown. A login account group must have *Manage Computers* privileges for its members to perform an emergency lockdown.

### Notes

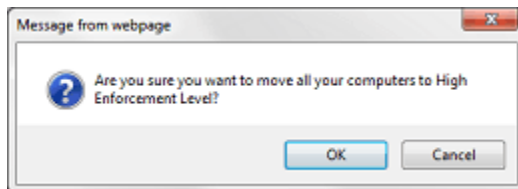
Emergency Lockdown changes only the *Enforcement Level* of computers. In policies with Advanced Settings of *Off* or *Report Only*, computers might not block certain threats even when in lockdown.

**To lock down all computers:**

1. From the console menu, choose **Home**. The Home page appears. The default location of the Emergency Lockdown portlet is the bottom right portlet on the page, although you or another administrator may have moved or removed it:



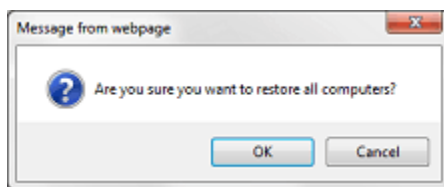
2. In the Emergency Lockdown portlet, click the **Lock Down** button. The Lockdown confirmation page appears:



3. In the confirmation dialog, click **OK** to lock down all computers. All agents except those in Disabled mode are locked down. The Home page appears and the **Lock down computers** button toggles to **Restore computers**:



4. After you resolve the issue that lead to the Lockdown, click the **Restore computers** button to restore all computers to their former Enforcement Level. The Restore confirmation page appears:



5. In the confirmation dialog, click **Yes** to restore all computers.



## Deleting Policies

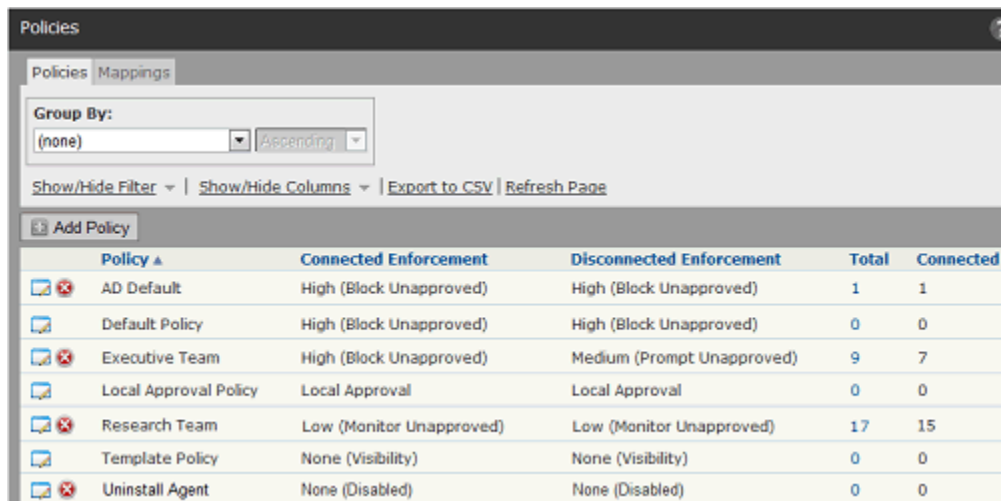
You can delete policies when you no longer need them. However, policies cannot be deleted if any computer is assigned to the policy. If a policy you want to delete has associated computers, either uninstall the Bit9 Agent on those computers or, to keep the computers protected by Bit9, move the computers to another policy. See “[Uninstalling Bit9 Agents](#)” on page 127 and “[Moving Computers to Another Policy](#)” on page 143. When you delete a policy, its associated agent installer is deleted from the Bit9 Server.

The following built-in policies cannot be deleted:

- Default Policy
- Local Approval Policy
- Template Policy

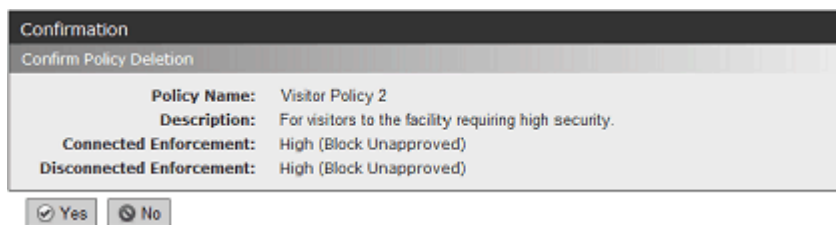
### To delete a policy:

1. On the console menu, choose **Rules > Policies**. The Policies page appears:



Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
AD Default	High (Block Unapproved)	High (Block Unapproved)	1	1
Default Policy	High (Block Unapproved)	High (Block Unapproved)	0	0
Executive Team	High (Block Unapproved)	Medium (Prompt Unapproved)	9	7
Local Approval Policy	Local Approval	Local Approval	0	0
Research Team	Low (Monitor Unapproved)	Low (Monitor Unapproved)	17	15
Template Policy	None (Visibility)	None (Visibility)	0	0
Uninstall Agent	None (Disabled)	None (Disabled)	0	0

2. On the Policies page, click the Delete (x) button next to the name of the policy you want to delete. A confirmation dialog appears.



**Confirmation**  
Confirm Policy Deletion

**Policy Name:** Visitor Policy 2  
**Description:** For visitors to the facility requiring high security.  
**Connected Enforcement:** High (Block Unapproved)  
**Disconnected Enforcement:** High (Block Unapproved)

Yes  No

3. Click **Yes**. You will return to the Policies page.

### Note

If a policy contains computers, clicking *Yes* in the confirmation dialog displays a deletion failure message on the Policies page. You must move these computers to another policy or delete them (on the Computers Page) before deleting the policy.



## Chapter 6

# Managing Virtual Machines

This chapter explains how the Bit9 Security Platform can efficiently manage virtual machines, called *clones* in the Bit9 Console, and the *template* computers on which they are based. To manage virtual machines, you also will need to be familiar with [Chapter 4, “Managing Computers.”](#)

### Sections

Topic	Page
<a href="#">Overview</a>	176
<a href="#">Creating a Template Computer</a>	177
<a href="#">Deploying Clones</a>	182
<a href="#">Making Changes to a Template</a>	184
<a href="#">Configuring Clone Inventory</a>	185
<a href="#">Deleting a Template</a>	185
<a href="#">Deleting Clones</a>	187
<a href="#">Converting a Template to a Regular Computer</a>	189

## Overview

When the Bit9 Agent is installed on a virtual machine, the Bit9 Security Platform can manage the virtual machine just as it manages physically distinct computers. However, you can *improve* the way virtual machines are managed if some special steps are taken.

When you provision a computer on a virtualized software platform that includes the Bit9 Agent and then convert that computer to a template using the Bit9 Console, much of the file inventory processing on clones based on this template can be optimized. The Bit9 Server can automatically initialize a clone's inventory based on its template, or optionally, you can choose to have the server track only file changes that happen after a clone is created.

These options reduce the network traffic and server load associated with cloned computers, potentially allowing much larger number of virtual machines to be managed by a Bit9 Server. In addition, the server maintains an association between the template and its clones so that you can easily discover which computers are based on a particular template and manage them accordingly.

### Notes

- While this chapter primarily describes how you manage virtual machines as clones, the procedures are applicable to re-imaging of physical computers (such as "ghosting") in which the clones are actually physical machines with a common disk image from a template.
- If you worked with Bit9 Technical Support to implement a custom solution to manage templates and clones in pre-7.0 Bit9 (Parity) releases, that solution will still work in version 7.2.1 but is not integrated with the new, standard template management features.

The following key terms are used throughout the chapter and in the Bit9 Console to describe the components of virtual and ghosted machine management:

- **Template Computer** - A computer that is pre-installed with required software, including the Bit9 Agent, and will be used to clone one or more computers through VMware or some other mechanism (e.g., "ghosting" of the hard drives of multiple computers from a common image). Before a computer can be used as a Bit9 template computer, it must be taken offline.
- **Cloned Computer** - A computer that originated as a clone of a template computer. It will register with the Bit9 Server as a new computer, but it will also remain identified as a clone of a specific parent template.
- **Parent Template** - Each cloned computer points to its parent Template Computer. This mapping persists until either the clone or the template is deleted.

The login account used to log in to the Bit9 Console must have Manage Computers permission to be able to manage templates and clones.

## Creating a Template Computer

The Bit9 Security Platform does not provide the software (such as VMware View) for creating virtual machines or managing cloned disk images for physical machines, nor does this chapter provide instructions for using those systems. A prerequisite of using the features described here is that you have, and know how to use, a product that creates clones from a master image. The Bit9 Server can manage the clones produced by those systems, but is not integrated with the systems themselves.

Bit9 requires the following for a template computer:

- it must have Bit9 (Parity) Agent 7.0.0 or greater installed
- it must *not* be the home of any Trusted Directories used by the Bit9 Server
- it must be fully initialized
- it can be either a physical computer or a virtual machine
- it must be shut down and show as *offline* in the console before becoming a Bit9 template computer, and should remain offline afterward

### To create a template computer:

1. On the computer you plan to use as a template, install the platform, application, and other files you want in the template image.
2. Install (or upgrade to) Bit9 Agent 7.2.1 or greater on the computer.
3. After Bit9 Agent installation, make sure the computer is connected to the Bit9 Server and let it fully initialize. You can monitor initialization progress by choosing **Assets > Computers** on the Bit9 Console menu and clicking on the View Details (pencil and file) button next to the name of the computer. Initialization progress is on the **Connection History** tab of the Computer Details page.


Bit9 Agent	Connection History	Policy Override	System Details	AD Details
<p>First Registered: Sep 27 2013 11:36:04 AM            Last Polled: Sep 27 2013 01:43:47 PM            Last Register Date: Sep 27 2013 01:43:40 PM  <b>Initialization: 23%</b>            Server Backlog: 70 files            Last Logged In User(s): MYCORP\SERVER-4\$                                              MYCORP\rjones</p>				

4. When initialization shows as *Complete*, also make sure that Synchronization is at 100%. Files added to the template computer after the Bit9 Agent is installed will be included in synchronization, not initialization. Wait for both initialization and synchronization are completed before proceeding to the next steps.

Bit9 Agent	Connection History	Policy Override	System Details	AD Details
<p>First Registered: Sep 30 2013 02:53:58 PM            Last Polled: Oct 4 2013 09:02:07 AM            Last Register Date: Oct 3 2013 01:58:09 PM  <b>Initialization: Complete</b>  <b>Synchronization: 100%</b>            Server Backlog: 0 files            Last Logged In User(s): MYCORP\SERVER-4\$                                              MYCORP\rjones</p>				

5. If you are using *sysprep* to prepare for creating an image of the template computer, go to the Computer Details page for this computer and disable tamper protection using the **Disable Tamper Protection** command on the Advanced menu. Refresh the Computer Details page until you see a value of *Tamper Protect: Disabled* on the Bit9 Agent tab.
6. Shut down the computer.
7. Go to the Computer Details page for the computer, and click **Convert to Template** on the Advanced menu. The Computer Details page changes to a Template Details page.
8. By default, the Template Name is the name of the computer from which the template was created, but you can change it, add a description, and change the cleanup and inventory parameters on the Template Settings tab (see [“Deleting Clones”](#) and [“Configuring Clone Inventory”](#) for details).
9. When you are satisfied with the configuration on the Template Details page, click **Save**. The computer now appears in the Computers table as a template.  
**Note:** Except for specific tasks described later in this chapter, you should not bring a computer back online after it is converted to a template. If you bring a template computer back online, it will appear as a clone of itself.
10. Create clones from the computer using your virtualization software. They will appear as new computers in the Bit9 Console.

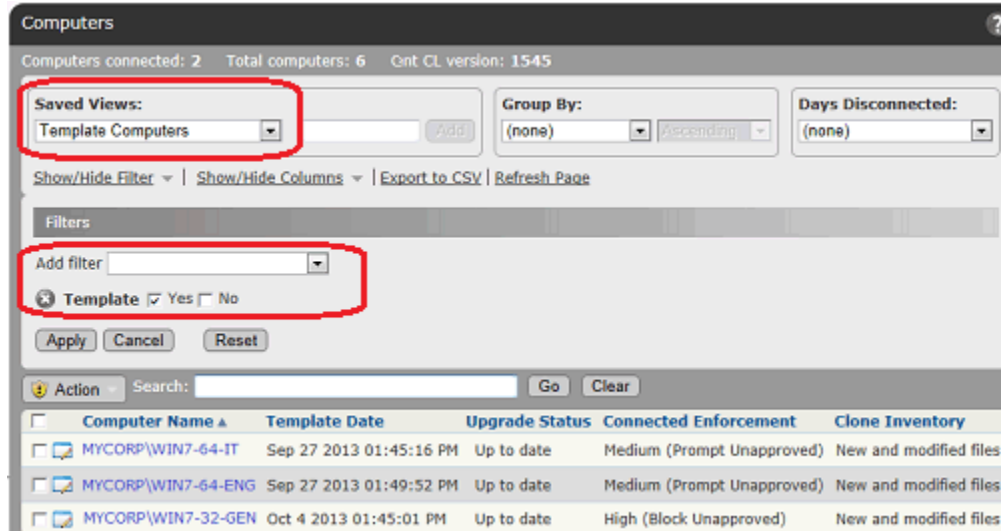
## Viewing Templates in the Computers Table

On the Computers page, you can view a table of computers and information about them, including their policies, Enforcement Levels, and whether they are currently connected to the server. By default, the full Computers table includes a Connected column, which indicates template computers by a white circle with a gray border . You also can add a Template column to the Computers table using the Show/Hide Columns button. This column will show *Yes* for templates and *No* for computers that are not templates.

If all you want to see is template computers, you can use the Template Computers Saved View.

**To view the template computers in the table of computers:**

1. In the console menu, choose **Assets > Computers**. The Computers page appears.
2. Choose **Template Computers** on the Saved Views menu to see computers that are templates for cloned computers.



3. The Saved View uses the filter checkbox *Template/Yes*. Instead of (or in addition to) the Saved View, you can click on **Show/Hide Filter** to further customize the view you have of the Computers table.

The default Template Computers view includes a Clone Inventory column that shows whether the file inventory of clones from this template includes all files on the clone computers or just files that were added or modified after creation of the clone. Note that the file inventory might also be affected by exclusion of tracking for Microsoft-signed support files. See [“Excluding Tracking of Microsoft Support Files”](#) on page 198 for details.

## Viewing and Editing Template Details

As with non-template computers, there are several ways to locate a template computer and display its details. You can use the Find Computer portlet on the Home Page to locate the template computer and then drill down to its details. The following procedure describes how you can locate and get details for a template computer through the Computers page.

**To view the Template Details page for one computer:**

1. In the console menu bar, choose **Assets > Computers**. The Computers Page appears.
2. In the Computers table, locate the template computer for which you want complete details (for example, searching by name, using the *Template Computers* Saved View, or using the Computer filters panel).

3. In the table, click either the name of the template computer or the View Details button next to its name. The Template Details page appears.

**Template Details**

**General**

Template Name: MYCORP\QA-TEMPLATE-IMAGE

Health Check: Passed

Platform: Windows

Description:

Computer Tag:

**Policy**

Policy: Engineering

Policy Mode: Control

Connected Enforcement: Medium (Prompt Unapproved)

Disconnected Enforcement: Medium (Prompt Unapproved)

**Template Settings**

Date Created: Sep 27 2013 01:45:16 PM

Original Computer Name: MYCORP\QA-DESKTOP-5

Original IP Address: fe93:b9:210:0:893:14dc:b269:f289

Clone Count: 4 online, 0 offline

Clone Inventory:  All files  New and modified files

Specify method for deleting of offline cloned computers...

Clone Cleanup: When offline

Save Cancel

**Related Views**

- Recent Events
- Health Check Events
- Files on this Computer
- Show all Cloned Computers

Much of the information is the same as for the Computer Details page (Table 15 on page 134), but there are important differences, as shown in Table 23.



**Table 23:** Differences between Template Details and Computer Details

Field/Menu/Tab	Description in Template Details Page
<b>Template Name</b>	Replaces Computer Name on the details page. By default this is the name of the computer from which the template was made. Must be unique.
<b>IP Address</b>	Not present on the Template Details page (has no meaning for a computer that is required to be offline).
<b>Connection Status</b>	Not present on the Template Details page (has no meaning for a computer that is required to be offline).
<b>Health Check</b>	On the Template Details page, this is the last Health Check done before the computer became a template.
<b>Policy Override tab</b>	Not present on the Template Details page.
<b>Template Settings tab</b>	<p>Details about the template. It includes the following:</p> <ul style="list-style-type: none"> <li>• <b>Date Created</b> – When the template was created in the Bit9 Console.</li> <li>• <b>Original Computer Name</b> – The name of the computer when it was converted to a template.</li> <li>• <b>Original IP Address</b> – The IP address of the computer when it was converted to template.</li> <li>• <b>Clone Count</b> – The current number of clones from this template.</li> <li>• <b>Clone Inventory</b> – Whether the file inventory for each clone should include all files, including the files cloned from the template computer, or only new and modified files. See <a href="#">“Configuring Clone Inventory”</a> on page 185.</li> <li>• <b>Clone Cleanup</b> – When clones for this template should be deleted when offline. See <a href="#">“Deleting Clones”</a> on page 187.</li> </ul>
<b>Related Views menu</b>	<p>Includes:</p> <ul style="list-style-type: none"> <li>• <b>Show All Cloned Computers</b>, which shows all clones for this template that have been connected to the Bit9 Server and not yet deleted.</li> <li>• <b>Health Check Events</b> shows the table of Health Check events for this computer before it became a template.</li> <li>• <b>Files on this Computer</b> takes you to a Find Files page with a table of all tracked file instances on the template computer.</li> </ul>
<b>Actions menu</b>	<p>The single item on this menu changes depending upon conditions:</p> <p><b>Delete Offline Clones</b> - Appears if the template has clones listed in the console. Deletes all clones of this template that are currently offline.</p> <p><b>Convert to Computer</b> - Appears if the template has no clones managed by the Bit9 Server. In this case, you can convert the template computer back to a regular computer and reconnect it to the server, if needed. This is primarily intended to allow you to undo an unintended template conversion.</p> <p>The menu does not appear if neither condition applies.</p>
<b>Advanced menu</b>	Not present on the Template Details page.

## Deploying Clones

Once you have registered a computer as a template, any clones of that template are automatically recognized by the Bit9 Server. Because they are clones, initialization will occur much faster than it would for non-clone computers.

Any manual or automatic methods of reverting the clones to their snapshot images will result in new clones being added to the console Computers list, still associated with the same template. The “old” clones go offline as far as the Bit9 Server is concerned, and they can be cleaned up by whatever method you choose (see “[Deleting Clones](#)” on page 187).

## Viewing Clones in the Computers Table

On the Computers page, you can view a table of computers and information about them, including their policies, Enforcement Levels, and whether they are currently connected to the server. You also can add a Parent Template column to the Computers table using the Show/Hide Columns button. Any computer that has a value in this column is a clone. Computers that are not clones show nothing in this column.

If you only want to see clones, you can use the Cloned Computers Saved View on the Computers page to see all cloned computers known to the Bit9 Server. By default, this view is grouped by Parent Template, so you know what the clones are based upon.

The screenshot shows the 'Computers' page in the Bit9 Security Platform. At the top, it displays 'Computers connected: 182', 'Total computers: 230', and 'Current CL version: 147122'. Below this, there are controls for 'Saved Views' (with 'Cloned Computers' selected), 'Group By' (set to 'none'), and 'Days Disconnected' (set to 'none'). There are also buttons for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', and 'Refresh Page'. A 'Filters' section shows 'Add filter' and a selected filter 'Parent Template is not empty'. Below the filters are 'Apply', 'Cancel', and 'Reset' buttons. The main table has columns for 'Computer Name', 'Connected', 'Policy Status', 'Connected Enforcement', 'IP Address', 'Policy', and 'Inventory'. The table is grouped by 'Parent Template' and shows several entries, including 'MYCORP\IT-VM2', 'MYCORP\IT-VM3', and 'MYCORP\IT-VM5'. At the bottom, it shows '10 items in 4 groups', 'Page 1/1', and '25 rows per page'.

Computer Name	Connected	Policy Status	Connected Enforcement	IP Address	Policy	Inventory
Parent Template: MYCORP\WIN7-64-IT 3 items						
MYCORP\IT-VM2	●	Up to date	Medium (Prompt Unapproved)	10.0.4.4	IT Group	All files
MYCORP\IT-VM3	●	Up to date	Medium (Prompt Unapproved)	10.0.4.5	IT Group	All files
MYCORP\IT-VM5	●	Up to date	Medium (Prompt Unapproved)	10.0.4.24	IT Group	All files
Parent Template: MYCORP\WIN7-64-ENG 1 item						
Parent Template: MYCORP\WIN7-32-GEN 5 items						
Parent Template: MYCORP\WIN7-32-ENG 1 item						

The Saved View for Cloned Computers uses the filter *Parent Template is not empty*. Instead of (or in addition to) the Saved View, you can click on Show/Hide Filter to further customize the view you have of the cloned computers.

The default Cloned Computers view includes an Inventory column that shows whether the file inventory of this clone includes all files (including those in the template image) or just files that were added or modified after creation of the clone.

## Finding the Clones for a Template

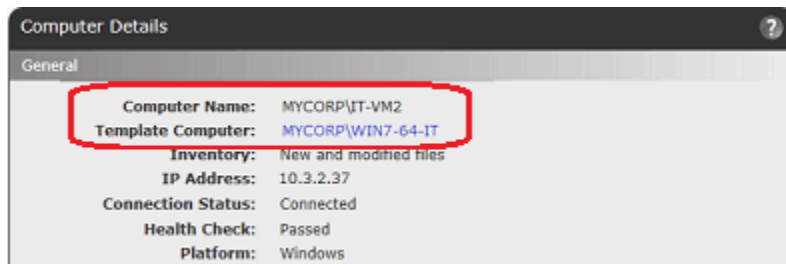
There are several ways to identify the clones created from a template:

- On the Computers page, you can choose the Cloned Computers Saved View. This displays clones grouped by their Parent Template.
- On the Template Details page, you can choose Show All Cloned Computers on the Related Views menu.
- On the Computers page, you can use the Parent Template filter to locate all clones from a particular template. This is also useful if you are not sure of the exact template name, since you can enter partial strings to match the name.

## Finding the Template for a Clone

You can find the template for a clone computer in the following ways:

- On the Computers page, you can choose the Cloned Computers Saved View. This displays clones grouped by their Parent Template.
- On the Computer Details page, the information listed for a clone is almost the same as the information listed for any other computer, but in addition to the standard information, there is a Template Computer field if the computer is a clone.



## Server Backlog for Clones

The Connection History tab on the Computer Details page includes a field called Server Backlog. This is the number of files that have been received from the computer but not yet fully processed on the server. Files in backlog appear in the File Catalog but not in the Files on Computers tab or Find Files page.

This is particularly significant for clones that are configured to inventory all files, including those in the template image. When a clone is discovered by the Bit9 Server, if it is configured to inventory all files, the file inventory from its parent template is copied into that computer's backlog. In this case, the Server Backlog field will show a large increase in the number of files. The file inventory of the cloned machine will not be available until this backlog is cleared.

## Making Changes to a Template

You might need to modify an existing template for all users, for example, to install new operating system updates. Another possibility is that you might need to keep the original template image but create a new template that is slightly modified to be appropriate for a different purpose or a different group of users.

To modify an existing template, you will have to bring the template computer back online. When it is online, it will be treated as a new clone computer of the original template. You can install updates and make any other needed modifications on the computer while it is considered a clone. When you are finished, you can convert the “clone” into a template. New templates made from an existing template computer automatically inherit the clone cleanup parameters from the original template.

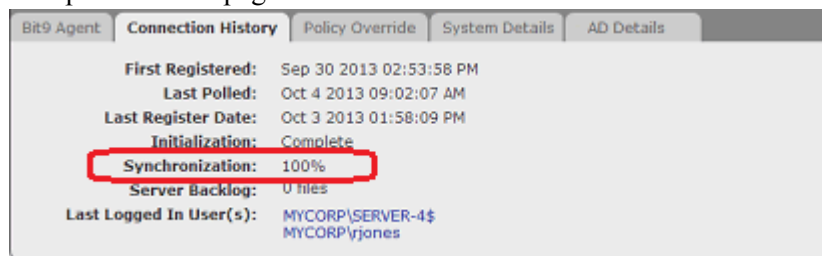
Clones of original template are not automatically deleted – they are still valid as long as they remain online. You can use your virtualization/imaging infrastructure to manage these clones as you see fit.

What you do with the old template depends upon why you updated it and whether there are still online clones associated with it. If the new template was truly an update and the old version is obsolete, you could delete the old template, preferably after any of its clones are offline. See [“Deleting a Template”](#) for more information.

If the new template was a variation, and not necessarily a replacement of the old template, you might want to keep both templates available.

### To update a template computer:

1. Bring the template computer back online. It will appear in the console as a clone of its original template.
2. On this “clone” computer, make whatever file additions, deletions and modifications you want for the updated template.
3. Using your virtualization or imaging software, update the image for this computer or create a new one.
4. Wait for the file inventory of the clone to be fully synchronized. You can monitor synchronization progress by choosing **Assets > Computers** on the Bit9 Console menu and clicking on the View Details (pencil and file) button next to the name of the computer. Synchronization progress is on the **Connection History** tab of the Computer Details page.



5. When Synchronization is 100%, shut down the computer or remove it from the network.

6. Go to the Computer Details page for the *clone computer you just updated* (not the original template), and click **Convert to Template** on the Advanced menu. The Computer Details page changes to a Template Details page.
7. The default name of the updated template is the old template name with a number appended to it to indicate how many times it has been updated. For example, if the original template was MYCORP\WIN7-64-IT, the edited template would be MYCORP\WIN7-64-IT (1), the next edited version would be MYCORP\WIN7-64-IT (2), and so on. You can change the name if necessary.
8. Create clones from the new template computer using your virtualization software.

## Deleting a Template

You can delete a template at any time. If you delete a template that has clones, those clones become freestanding computers; that is, they lose their association with the template. Even if you restore the template computer at a later time with the same name, the clones do not reconnect with it.

### To delete a template computer from the Bit9 Console:

1. On the console menu, choose **Assets > Computers**.
2. Locate the template computer using the Template Computers view or some other method.
3. In the Computers table, check the box next to the template computer, choose **Delete Computers** from the Action menu, and confirm the deletion.

#### Note

If a template has no clones, you also can convert it to a regular (non-template) computer and manage it with the Bit9 Server. See [“Converting a Template to a Regular Computer”](#) on page 189.

## Configuring Clone Inventory

A primary reason to use Bit9’s virtual machine management features is to optimize file inventory processing on future clones created from a template computer. There are two options for clone file inventory management:

- **All files** – The Bit9 Server can automatically initialize a clone's file inventory based on the files present on the template. As soon as a clone is detected, the inventory from its template is copied into the clone’s inventory. Any future file additions or changes are also applied to the clone inventory. This is the default setting.
- **New and modified files** – You can choose to have the clone start with an empty file inventory and have the server track only file additions and changes for each clone that happen after it is created.

These options are set on a per-template basis. They affect how the Files on Computers inventory for *clones* are managed. Regardless of your choices here, all files from the template image are included in the Bit9 File Catalog on your server.

If you choose *New and modified files*, the clone inventory will track the following changes from the baseline template inventory:

- creation of a file
- modification of a file
- deletion of a file
- renaming of a file
- changes in a file's Bit9 state (i.e., approvals and bans)

Changes in the *path* for a file (other than a change in the file name itself) will not cause a file that was in the template inventory to be tracked as part of the clone inventory.

## Choosing an Inventory Option

The best choice for clone inventory will depend upon your environment and your priorities. The most obvious advantages of choosing to inventory only new and modified files are a reduction in network and server traffic and minimization of data that might not be of interest to you. This can be particularly important in an environment with thousands of cloned computers and a large base image of files.

This should be balanced against the impact of limiting the clone inventory. If new and modified files is chosen:

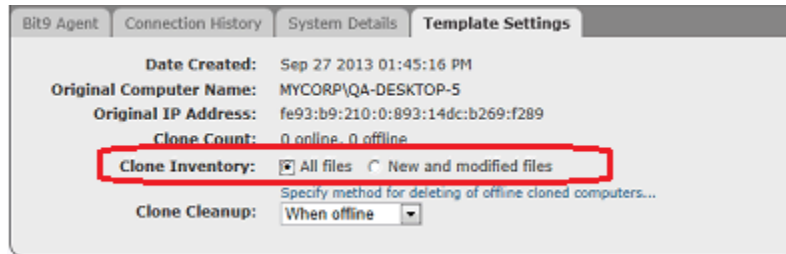
- Neither the Find Files page nor the Files on Computers page will be able to show all files on a clone computer.
- Drift reports that involve cloned machines will be incomplete. The only type of drift reporting that will work correctly is self-drift (comparison of the files currently on the clone computer with its own previous inventory), and unmodified files from the initial template image will not be included in this report.
- Snapshots created from cloned computers will include only new and modified files.
- File prevalence will not be accurate for unmodified files from the template image because instances on clones will not be counted (and also deletion of files from the original image will not be accounted for).
- Because unmodified files in the template image will not be visible in the clone computer's inventory, direct local approval of such files will require that the specific file instance (on the specific clone computer) appears in an event. Otherwise, global approval might be required.

### Note

Bit9 also provides an option to exclude tracking of certain Microsoft-signed operating system and application files, and this can significantly reduce traffic and database demands. This affects all computers, not just clones. See [“Excluding Tracking of Microsoft Support Files”](#) on page 198 for more details.

**To configure the clone inventory setting for a template:**

1. On the console menu, choose **Assets > Computers**.
2. Locate the template computer using the Template Computers view or some other method, and click on the View Details button or the computer name.
3. Click on the **Template Settings** tab.



4. In the Clone Inventory field, choose the radio button for either **All files** or **New and modified files**.
5. If you have no other configuration changes, click **Save**.

**Note**

Even if you choose *New and modified files* for the inventory option, if a clone goes offline and then a clone with the same name is connected after its files are marked as deleted, the server will do a full inventory, including the files provided as part of the template image.

## Deleting Clones

If you create and retire virtual machines on demand in the environment managed by the Bit9 Security Platform, you will want to make sure that old clones no longer in use do not remain on the Computers page. For example, you might have virtual machines automatically revert to their snapshot on a timed basis or every login, or you might frequently update the template image for your clones. The Bit9 Security Platform offers several ways of cleaning up old clones.

- **Manual cleanup** – If you choose, you can leave all cleanup to manual methods, periodically deleting offline clones through the Template Details page.
- **Automatic cleanup for all clones** – You can configure a cleanup rule that deletes offline clone computers on a schedule. You can delete *all* offline clone computers or only those matching a particular filter. For example, you could delete all computers that are running in a virtualized environment and are offline for more than 5 days.
- **Automatic cleanup per template** – You can configure different cleanup rules for different templates.

As with regular, non-clone computers, the file inventory for a deleted clone is deleted 24 hours after the clone is deleted.



## Manual Cleanup of Clones

There are two primary methods of manual clone cleanup:

- You can locate a particular clone through the Cloned Computers Saved View and delete it as you would any other computer.
- You can go the Template Details page for a template and use the Delete Offline Clones command in the Action menu.

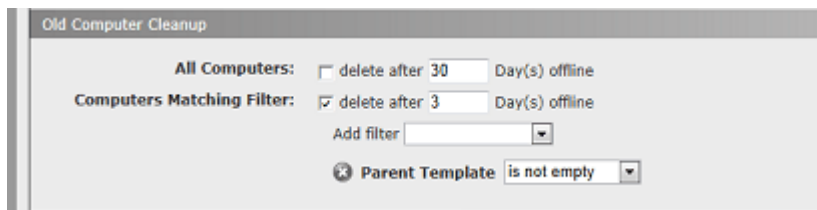
## Automatic Cleanup for All Clones

The Advanced tab of the System Configuration page includes settings that remove offline computers from the list of managed computers. You can either choose to remove *any* computer from the console after it is offline for a certain period of time or you can set filters that selectively remove computers.

If you leave the Clone Cleanup configuration for each template on Manual, you can use the filtered global cleanup methods to remove offline clones. If you set an automatic cleanup method for one or more templates and set one of the global removal methods, offline clones will be removed whenever they meet *either* rule.

### To create a global cleanup rule for offline clones:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Advanced Options** tab. The Advanced Options configuration page appears.
3. Click the **Edit** button.
4. In the Old Computer Cleanup panel, configure Computers Matching Filter to delete clone computers after an amount of time you specify:
  - a. Check the box to the right of Computers Matching Filter.
  - b. Enter the number of days offline after which you want the computers deleted from the console Computers page.
  - c. On the Add Filter menu, choose an appropriate filter. For example, choose **Parent Template** and in the menu that appears next to Parent Template, choose **is not empty**. This assures that any computer with a template will be deleted. You also can choose **Virtualized** and check the Yes box to cleanup all virtual machines (whether or not they are clones) but not any clones created by other means. Or, you can choose **Virtual Platform** and enter **VMware** in the field to cleanup VMware computers.



5. To save the changes, click the **Update** button and click **Yes** on the confirmation dialog.



## Automatic Clone Cleanup for One Template

Each template has its own clone cleanup setting. You can choose manual cleanup or one of two automatic settings. If you also set a global clone cleanup rule on the System Configuration pages, templates are also subject to that rule.

### To configure automatic clone cleanup for a specific template:

1. On the console menu, choose **Assets > Computers**.
  2. Locate the template computer you want to configure for clone deletion and click its View Details button to open the Template Details page.
  3. Click on the **Template Settings** tab. It shows when the template was created, the computer's original name and IP Address, and how many clones from the template have been seen by the Bit9 Server. It also includes a menu on which you can choose how to cleanup clone computers for this template.
  4. On the Clone Cleanup menu, you can choose one of the following:
    - **Manual** - No automatic cleanup. Clones based on this template must be deleted manually, or by the global cleanup rule defined on the System Configuration Advanced tab.
    - **When offline** - Clones based on this template are scheduled for deletion as soon as they are offline. Depending upon other server activities, they will actually be deleted within 10 to 15 minutes.
    - **Based on time** - Clones based on this template are deleted if offline for a period of time you set in a field that appears when you make this choice. If there are two different times defined for the template and for global cleanup, the first deadline to be reached triggers the cleanup.
    - **Based on name** - When a clone based on this template is newly registered with the Bit9 Server, any *offline* clones with the same name are automatically deleted. Online clones are not affected. This method is safe to use unless you want to retain old reverted computer data for analysis. This will not cleanup offline clones if new clones always get a new name.
- Note:** To prevent accidental deletion of clones that are still in use, clones that are detected as offline will not be deleted unless they have not communicated with the server for at least 10 minutes. This helps mitigate situations in which network interruptions erroneously make it appear that a clone is not in use.
5. When you have completed any changes you want to make to the Template Details page, click **Save**.

## Converting a Template to a Regular Computer

You can convert a template back to a regular computer. This feature is primarily intended as a remedy in case you accidentally convert a computer to a template. However, you can use it for any reason. If you want to convert a computer that was actually used as a template, you should make sure it does not have any clones listed on the Computers page in the Bit9 Console before the conversion.

**To convert a template computer back to a regular, agent-managed computer:**

1. On the Template Details page for this template, click on **Show all cloned computers** in the Related Views menu.
2. If there are any clones listed for this computer, delete them from the Bit9 Server or leave the template in place as a template (see [“Deleting Computers”](#) on page 146). Otherwise the clones become freestanding computers (i.e., with no connection to a template).
3. When you have made certain that the template has no clones, return to the Template Details page and click **Convert to Computer** in the Action menu. The computer returns to Bit9 Server management and the Template Details page is converted to a Computer Details page.
4. After the conversion is complete, reconnect the computer so that the server can manage it.

## Chapter 7

# File and Publisher Information

This chapter describes the location and contents of information available for files discovered and managed by the Bit9 Security Platform, as well as information about the publishers associated with these files. It also describes options that exclude tracking of certain files and show all computers with or without certain files.

### Sections

Topic	Page
<a href="#">Overview</a>	192
<a href="#">File Catalog</a>	193
<a href="#">Files on Computers</a>	195
<a href="#">Showing Individual Files</a>	195
<a href="#">Finding Computers With or Without Specified Files</a>	197
<a href="#">Excluding Tracking of Microsoft Support Files</a>	198
<a href="#">File Groups</a>	202
<a href="#">File Details Page</a>	204
<a href="#">File Instance Details Page</a>	210
<a href="#">Summary of File Views</a>	215
<a href="#">Global File State</a>	217
<a href="#">Local File State</a>	218
<a href="#">Publisher Information</a>	220

## Overview

The Bit9 Security Platform collects many different kinds of information about the “interesting” files it discovers on your computers. Interesting files are files that are either determined by the Bit9 Platform to be executable (for example, .EXE or .DLL files) or that match file extensions defined as scripts. You can use this information simply to be aware of the file activity, or to make decisions about how you want to control execution and writing of particular files or classes of files.

Many files discovered by the Bit9 Agent have an identified *publisher*. As with other file information, the publisher can be useful simply to know where a file came from, or it can be used to automatically approve or ban files.

### Notes

Some file and publisher information is provided by the Bit9 Software Reputation Service (SRS). You must have Bit9 SRS activated to receive this information. See [“Activating Bit9 SRS”](#) on page 643 for more information.

For information about using file and publisher information to approve or ban files, see [Chapter 8, “Approving and Banning Software.”](#)

File information is presented in table form in several locations within the Bit9 Console, but the primary starting point is the Files page, which you access by choosing **Assets > Files** on the console menu. The Files page has two tabs:

- The **File Catalog** tab shows the unique “interesting” files discovered on your computers. Cataloged files includes those currently present and tracked on agent computers, files considered “interesting” but not tracked in inventory, and files that were once present on an agent system but have been deleted.
- The **Files on Computers** tab shows tracked file instances. This includes every instance of every “interesting” file on every agent-managed computer reporting to your Bit9 Server (once their files are fully processed), with these possible exceptions:
  - You can exclude common Microsoft operating system and application support files from the file inventory to reduce tracking overhead and database size. See [“Excluding Tracking of Microsoft Support Files”](#) on page 198 for details.
  - You can exclude instances of files that are in the template used by a VDI product to create a clone. See [“Configuring Clone Inventory”](#) on page 185 for details.
  - You can disable file tracking on a policy-by-policy basis.

If any of these conditions affects files on your computers, the Prevalence value for those files will not be accurate -- only tracked files can contribute to Prevalence.

For complete information about one file in a table, you can go to a details page for the file:

- The **File Details** page shows the global information about one unique file and provides a link to a list of all instances of that file.
- The **File Instance Details** page shows information about a specific file instance on a specific computer.

Publishers for files discovered on agents managed by your Bit9 Server are shown in the table on the Publisher rules page, which you access by choosing **Rules > Software Rules** and clicking the **Publishers** tab on the console menu. If you want complete information about one publisher in the table, you can go to the details page for the publisher.

# Viewing File Tables

## File Catalog

The File Catalog tab on the Files page shows unique files discovered on computers running the Bit9 Agent in your organization. In addition to displaying tables of files and their details, the File Catalog page includes an Action menu that allows you to take a variety of file-related actions, including approving, banning and looking up information about them in Bit9 Software Reputation Service. These actions are described in other chapters.

From the File Catalog, you can open a File Details page by clicking on the View Details (file and pencil) button next to a file name. The column headings available in the File Catalog correspond in most cases to fields on the File Details page for a single file. See [Table 25, “File Details and File Catalog Page Fields,”](#) on page 205 for a description of this information.

The screenshot shows the 'File Catalog' tab in a web application. At the top, it says 'Files: All Unique Files'. Below that, there are tabs for 'File Catalog' and 'Files on Computers'. There are controls for 'Saved Views' (currently '(none)'), 'Group By' (currently '(none) Ascending'), and 'Max Age' (currently 'None'). Below these are links for 'Show/Hide Filter', 'Show/Hide Columns', 'Show/Hide Snapshot', 'Export to CSV', and 'Refresh Page'. An 'Action' menu is visible above a table of files.

	First Seen Date	First Seen Name	Publisher or Company	Product Name	Trust	Global State
<input type="checkbox"/>	Nov 29 2011 10:00:25AM	googleupdatesetup.exe	Google Inc.	Google Update	10	Approved
<input type="checkbox"/>	Nov 20 2011 04:56:34PM	solsuite.exe	TreeCardGames.com		8	Unapproved
<input type="checkbox"/>	Nov 19 2011 11:03:24AM	crashreporter.exe	Mozilla Corporation	Firefox	10	Approved
<input type="checkbox"/>	Nov 19 2011 11:03:24AM	brwsrcomp.dll	Mozilla Corporation	Firefox	10	Approved
<input type="checkbox"/>	Nov 16 2011 09:14:48AM	swdir.dll	Adobe Systems Incorporated	Shockwave	10	Approved

By default, the File Catalog shows all unique *top-level* files (files not known to have been installed by or copied from another file). You can choose a different Saved View of the catalog or create a view of your own to focus on particular types of files or search for one file. If you have not already become familiar with modifying views in console tables, see [“Bit9 Console Tables”](#) on page 58. You also can choose to show all individual unique files instead of top-level files only. See [“Showing Individual Files”](#) on page 195 before choosing this option.

### Note

The File Catalog shows the First Seen Name of a unique file, and the unique file is identified by its hash. The name used for a file instance *on a particular computer* might not appear in the File Catalog even though it appears in the Files on Computers tab. Use Find Files or the Files on Computers tab to locate a particular instance by name.

[Table 24](#) shows the Saved Views provided on the File Catalog tab.

**Table 24:** Saved Views on the File Catalog tab

Saved View	Description
<b>Applications by Publisher/Company</b>	Files that are identified as Applications or Packages, and, in this view, are grouped by their Publisher (if available) or Company.
<b>Approved Files</b>	All executable files approved by a Bit9 global approval method.
<b>Banned Files</b>	All files explicitly banned by hash. Files banned by name do not appear in the table on the File Catalog tab. Files that are banned for some policies but not others do not appear in the Banned Files table, but can be found in the File Catalog tab by using the File State filter.
<b>Categorized Files</b>	Files that exist on at least one computer and fall into one of the application categories identifiable by Bit9 SRS (such as Hacking Tools and Instant Messaging). In this view, the files are grouped by category.
<b>Existing Files</b>	Files that exist on at least one agent-managed computer on your network.
<b>Installed Programs</b>	Files grouped by the installed program with which they are associated. This view shows the full package or application name for the installed programs. <b>Platform Note:</b> Only Windows files are identified as Installed Programs
<b>Malicious Files</b>	Files that exist on at least one computer and have been identified by Bit9 SRS as having a Threat level of 1-Potential risk, or 2-Malicious.
<b>New Unapproved Files</b>	Unapproved files that appeared on computers <i>after</i> file initialization, that have not been Acknowledged, and that still exist on at least one computer.
<b>Removed Files</b>	Files that no longer exist on any agent-managed computer reporting to your Bit9 Server.
<b>Reputation Approvals</b>	Files that have been approved because of the trust rating of the file or its publisher in Bit9 SRS.
<b>Trusted Packages</b>	Top-level files, located in a Trusted Directory, that are the common source or installer files for other files. Click the View Details button to display the File Details page for the package itself. Click on the package name for a table of associated files written by the package. Note that the root file for each package may also appear in other tabs.

## Files on Computers

The Files on Computers tab provides a table of files that are on agent computers or, for disconnected computers, were on those computers when their agents last communicated with the Bit9 Server. Files from deleted computers may continue to appear for one day but will be marked as being from a deleted computer during that time and will no longer appear after the grace period.

By default, the Files on Computers table shows *all* top-level files (files not known to have been installed by or copied from another file) on all computers, plus groups of initialized files (i.e., files on a computer when the Bit9 Agent was installed). You can choose a different Saved View of the catalog, however, or create a view of your own to focus on particular types of files or search for one file. If you are not already familiar with modifying views in console tables, see “[Bit9 Console Tables](#)” on page 58. You also can show individual files on computers instead of top-level files only. See “[Showing Individual Files](#)” before choosing this option.

The Files on Computers tab includes the following subset of the Saved Views shown in [Table 24](#), “[Saved Views on the File Catalog tab](#)” on page 194:

- Applications by Publisher/Company
- Banned Files
- Categorized Files
- Installed Programs
- Malicious Files
- Unapproved Files

[Table 25](#) shows the fields that can appear in the File Catalog table, most of which also can appear in the Files on Computer table. [Table 26](#) shows additional fields that are available on the Files on Computers tab. Note that not all fields appear by default.

## Showing Individual Files

The checkbox labeled *Show individual files*, in the bottom right of both Files page tabs, has a major effect on what files are shown.



When *not* checked (the default), the File page shows only top-level files (files *not* known to have been installed by or copied from another file). On the Files on Computers page, it also shows groups of initialized files for each computer.

When this box *is* checked, the Files page shows top-level files *and* files installed by other files. A complete File Catalog listing of the unique files reported to the Bit9 Server might number in the tens of millions. Files on Computers, which is an inventory of files actually on your computers, can be significantly larger. In rare cases, especially with a particularly large number of Bit9 Agents and/or an underpowered database server, attempting to show all individual files can cause the Bit9 Server to time out. In that case, consider modifying the view. For example, you could turn off *Show individual files*, change the *Group by* choice, or sort by a different column. You also can use a filter to limit the total number of files shown.

A possible side-effect of requesting a table with a very large number of files is that the number of items on all pages of the table, shown in the lower left corner, will show as an approximation, such as *More than 10000 items*. This can also occur if a view you request requires extra processing by the Bit9 Server, even if the number of results is not especially large. Clicking **Refresh Page** after the results are displayed often shows the exact number.

Keep in mind that you can click on the name of a top-level file in the File Catalog or Files on Computers page to get a list of the individual files associated with it.

**Platform Note:** For this release of the Bit9 Security Platform, only Windows files are grouped by installer, so checking *Show individual files* does not change the files shown from non-Windows computers in the File Catalog. On the Files on Computers tab, however, initialized files are grouped together, as are files from Mac packages (.pkg files with properly marked headers), so checking *Show individual files* does expose many more files in the table.

## Initialized Files

File *initialization* is the inventory of files that begins immediately after installation of the Bit9 Agent on a computer. The agent takes an inventory of all executable files on the client computer's fixed drives and creates a hash of each file. When a computer first connects to the server, its agent sends each hash to the Bit9 Server to update the server's file inventory. Files on a computer at initialization receive a *local* state of Approved unless they already have been identified and globally banned or banned by policy on the Bit9 Server.

For each agent-managed computer, there is a row with the file name **<Initialization files>** in the Files on Computers table when Show individual files is not checked. Clicking on **<Initialization files>** opens a table showing all initialized files for one computer. This is a useful way to determine what was on each system before the agent was installed.

Date Created	Computer	File Name	Publisher or Company	Trust	Threat
Nov 02 2012 03:57:26PM	MYCORP\DESKTOP-3	<Initialization files>			
Oct 30 2012 01:57:53PM	MYCORP\SERVER-1	<Initialization files>			
Oct 30 2012 10:12:21AM	MYCORP\DESKTOP-4	<Initialization files>			
Oct 30 2012 09:06:08AM	MYCORP\DESKTOP-4	bitcc6.tmp	Microsoft Corporation	10	✓
Oct 30 2012 09:08:35AM	MYCORP\DESKTOP-4	fileformatconverters.exe	Microsoft Corporation	10	✓
Oct 30 2012 09:06:01AM	MYCORP\DESKTOP-4	poqexec.exe	Microsoft Corporation	10	✓
Oct 30 2012 09:06:05AM	MYCORP\DESKTOP-4	trustedinstaller.exe	Microsoft Corporation	10	✓
Oct 30 2012 09:06:03AM	MYCORP\DESKTOP-4	wuauclt.exe	Microsoft Corporation	10	✓

If you disable and then re-enable an agent, a new initialization process begins, and the **<Initialization files>** group will change. Other than that, this group should not change unless there is a problem with the agent. Upgrading the agent does not change the list of initialized files.

When you click on **<Initialization files>** on the Files on Computers page, you get a file list for the computer shown in the table. If you click on one of the files, it will show a list of



Groups that contain the file but it will not identify the group containing it for the current computer. This is because a file that predates the agent may have been installed or copied from any one of a variety of places.

If you use a filter with `Initialized = Yes` on the Files on Computers page with the Show individual box not checked, the table shows rows for <Initialization files> and usually several other files. The other files are known installers, but are also included under the <Initialization files> group.

	Date Created v	Computer	File Name	Publisher or Company	Trust	Threat
<input type="checkbox"/>	Nov 05 2012 09:24:11AM	MYCORP\DESKTOP-3	11506f.msi	Microsoft Corporation	10	
<input type="checkbox"/>	Nov 02 2012 03:57:26PM	MYCORP\DESKTOP-3	<Initialization files>			
<input type="checkbox"/>	Oct 30 2012 01:57:53PM	MYCORP\SERVER-1	<Initialization files>			
<input type="checkbox"/>	Oct 30 2012 10:12:21AM	MYCORP\DESKTOP-4	<Initialization files>			
<input type="checkbox"/>	Oct 30 2012 09:08:35AM	MYCORP\DESKTOP-4	devenv.exe	Microsoft Corporation	10	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Oct 30 2012 09:06:08AM	MYCORP\DESKTOP-4	385fa53.msi	Microsoft Corporation	10	
<input type="checkbox"/>	Oct 30 2012 09:06:05AM	MYCORP\DESKTOP-4	trustedinstaller.exe	Microsoft Corporation	8	<input checked="" type="checkbox"/>

## Menus on the File Tables Pages

The File Catalog and Files on Computers tables have an Action menu in the upper left above the table. [Table 27, “Menus on File Tables and Details Pages,”](#) on page 214 shows the available choices on file page menus. Note that some choices are available only for certain file states.

## Finding Computers With or Without Specified Files

If you add an application to your environment or update an existing program with a new file, you might want to determine whether any computers are missing the file or files involved in this change. On the other hand, you might have found one or more files that you want removed from your environment. In that case, it would be helpful to be able to get a list of all computers that still have these files. The Files pages in the Bit9 Console include menu choices that provide this information, using the file hash as the search parameter.

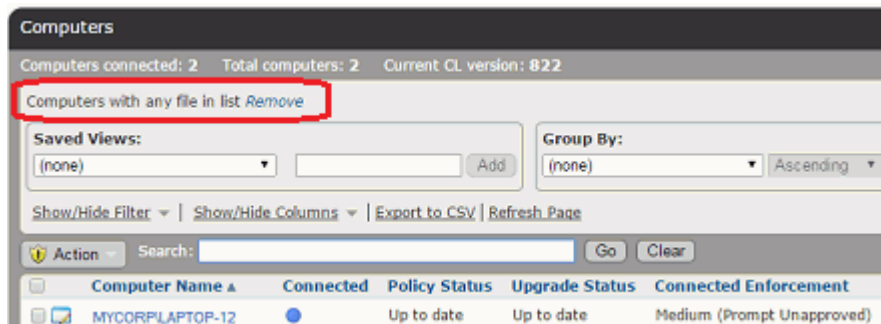
On the Related Views menu of both the File Details and File Details pages, you have the following computer-search options:

- **Computers with this file** -- Shows the Computers table with a list of all computers that have the file described on the details page.
- **Computers without this file** -- Shows the Computers table with a list of all computers that *do not* have the file described on the details page.

On the File Catalog, Files on Computers, and Find Files results pages, you can check multiple files in the table and apply Action menu commands to all of them. This provides more computer search options:

- **Find computers with at least one of the selected files** -- Shows the Computers table with a list of all computers that have at least one of the files checked on the Files page.
- **Find computers with all of the selected files** -- Shows the Computers table with a list of only those computers with *all* of the files checked on the Files page.
- **Find computers missing at least one of the selected files** -- Shows the Computers table with a list of all computers that are missing any of the files checked on the Files page.
- **Find computers missing all of the selected files** -- Shows the Computers table with a list of only those computers missing *all* of the files checked on the Files page.

When the Computers page shows the results of any of these commands, a legend appears above the Saved Views menu indicating what kind of command was used. If you want to eliminate the filtering that produces these results and instead view the standard Computers page view, click the **Remove** link next to this legend.



### Note

If a file has been excluded from the Files on Computers inventory, you cannot use these commands to locate computers with that file. For example, if tracking of Microsoft support files has been turned off on the Advanced tab of the System Configuration page, you cannot get accurate results for those files from any of the Find computers commands.

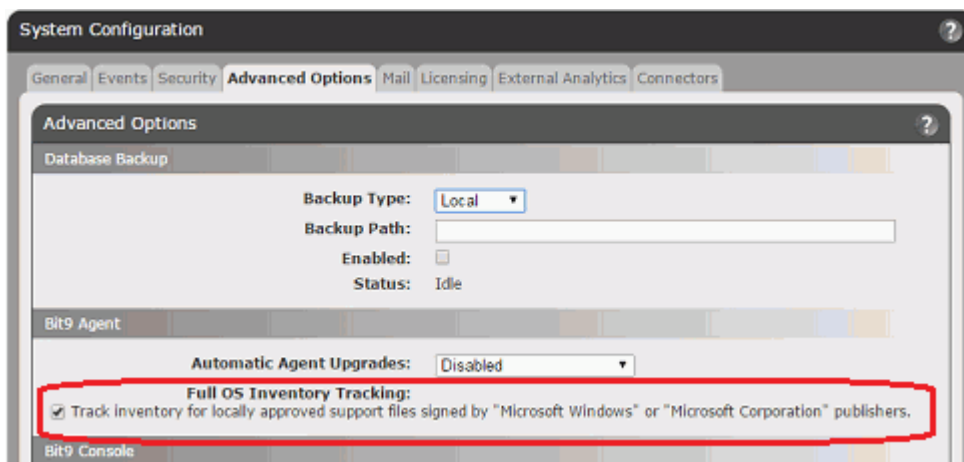
## Excluding Tracking of Microsoft Support Files

By default, Bit9 inventories and tracks all instances of interesting files on all agents attached to a server. Many of these files are Windows operating system and Microsoft application files and related system updates. As Windows has evolved, the number of operating system files has multiplied to several times what it was in Windows XP, and applications have had similar increases in file number. Windows updates are also significantly increasing in size. Because of these increases, Microsoft files may account for more than half and in some cases three-quarters of all of the files found in your inventory for Windows computers.

If you trust and approve files from Microsoft, you might also prefer not to track them. The Bit9 Platform provides an option that eliminates file tracking for certain files that have been signed by the publishers "Microsoft Windows" or "Microsoft Corporation". By turning off file tracking for a significant percentage of the file instances on your systems, you can reduce the size of the database needed for a given number of agents as well as reducing the load on the server that would be required to process these files.

Turning off tracking for these files excludes *instances* of them from the Files on Computers inventory and limits events related to them. This eliminates your visibility into these files on endpoints, but their hash and information about the file will appear in the File Catalog as long as they have appeared on one agent-managed computer. In addition, events related to these files, such as approvals and bans, continue to be reported.

Tracking of Microsoft-signed support file instances is controlled on the Advanced Options tab of the System Configuration page. By default, these files are tracked.



#### To disable or re-enable tracking of Microsoft-signed support file instances:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Advanced Options** tab, and at the bottom of the page, click the **Edit** button.
3. In the Bit9 Agent panel, *uncheck* the box for Full OS Inventory Tracking. This disables tracking of support files signed by "Microsoft Windows" or "Microsoft Corporation".
4. At the bottom of the page, click the **Update** button. Support file tracking is disabled.
5. To re-enable tracking of these files, check the Full OS Inventory Tracking box and click the **Update** button. If you are certain you want to make this change, click **Yes** on the Confirmation dialog.

**Note:** The Confirmation dialog for re-enabling Full OS Inventory Tracking includes a warning about possible effects on product performance. If you have been operating with this setting off for some time, consider whether your environment meets the requirements for significant additional file traffic.

## Files Instances Affected

When you turn off Full OS Inventory Tracking, instances of files meeting *all* of the following criteria are no longer tracked:

- The publisher is "Microsoft Windows" or "Microsoft Corporation". This includes directly signed files and those signed with a detached publisher. Files signed by other Microsoft publishers, even if legitimate, are not excluded from tracking.
- The file is a support file, such as a .DLL, that would normally be considered "interesting" and therefore be tracked by Bit9. Tracking of .EXE files or the events related to them is not affected by this option.
- The file is locally approved, either directly or because of an approval rule.

## Changes that Affect OS Inventory Tracking

As with other rules, there are interactions between the Full OS Inventory Tracking rule and several other rules and conditions in the Bit9 Platform:

- **File State Transitions** – If file exclusion is enabled (that is, Full OS Inventory Tracking is *disabled*), unapproved file instances that otherwise meet the exclusion criteria are inventoried and tracked. If these files are later approved, they will no longer be tracked, but the server will not incorporate their state change; they remain in inventory even though their prevalence will show as zero. Conditions that can cause this include:
  - A Microsoft support file was locally *unapproved* and so, not excluded from inventory, and later it was locally approved.
  - The criteria for publisher trust is high when Full OS Inventory Tracking is disabled (for example, minimum key size for approval is 2048), and so Microsoft support files are *not excluded*. Then, the publisher trust criteria is lowered (for example to a 1024-bit minimum), approving most of the support files.
- **Disabling Tracking** – If you disable Full OS Inventory Tracking, the following occurs:
  - All affected files are deleted from the file inventory on the Files on Computers page. Deletion will happen in the background, while the server is not busy, and could take several days to complete, depending on inventory size. An event will report how many files were deleted from the inventory.
  - New, approved instances of these files and changes to them will not be inventoried or tracked.
- **Re-Enabling Tracking** – If you re-enable Full OS Inventory Tracking after it has been disabled, there will not be an automatic re-inventory of Microsoft-signed files from agent computers. New instances or activity related to relevant files will be tracked. If you want to collect an inventory of all pre-existing Microsoft support files, you can Resynchronize all File Information on a computer-by-computer basis. This option is available on the Computers page Action menu.
- **Agent Version** – You can turn off tracking of Microsoft support files on both new 7.2.1 and (supported) older agents, but the behavior is different. The server cannot always exclude files from older agents immediately because it is missing some of the necessary information. For example, it will not always be able to detect that file is a supporting file, or that the file is signed by Microsoft. However, these files will be deleted in the background during a regular daily update of file information.

## Information about Excluded File Instances

Even if you turn off tracking of approved Microsoft support file instances, information about them is available. Some of this is generic information about the file itself, not its specific instances.

When you turn off tracking of locally approved support files signed by the two relevant Microsoft publishers, these files still appear in the File Catalog if a file with their hash has appeared on any agent monitored computer. Because instance tracking is turned off, the file Prevalence (the number of computers they are found on) number will not be reliable (and might be zero), and a tooltip will indicate that prevalence cannot be calculated.

Publisher or Company	Prevalence	Excluded from Inventory ▾	Product Name
Microsoft Corporation	Prevalence for this file is not accurate because file has been excluded from the inventory		
Microsoft Corporation	1	Yes	Assembly imported from type library *
Microsoft Corporation	1	Yes	Microsoft SQL Server
Microsoft Corporation	1	Yes	Microsoft SQL Server

It is possible that you will want to turn off tracking of these files in general but track specific instances, for example, if a particular version of a Microsoft DLL has a reported vulnerability and you want to replace it. There are several ways to maintain the general setting so that you can reduce the load from these files but also track executions of certain files:

- **Report Bans** – You can create a report-only ban for a file. This will cause all instances of this file on all computers to be added to the inventory.
- **Meters** – If you create a Meter for a file hash, the meter will report all executions of an excluded file as events but not add instances of it to the Files on Computers inventory.
- **Exports of Data to Analytics Tools** – If you have integrated the Bit9 Platform with an External Analytics tool, such as Splunk, data from excluded file instances is included with all the other file and event data. You can use the external tool to find all instances of excluded files as they appeared historically on all computers, and executions of these files are also tracked in the data provided to the external tool.
- **Excluded from Inventory Column in File Catalog** – The optional column *Excluded from Inventory* is available in the File Catalog. If you add this to the table, it identifies files whose instances are not in the file inventory because they are excluded OS support files.  
**Note:** Files locally approved *after* Microsoft support file exclusion was activated will continue to appear as *unapproved* files and so appear in the Files on Computers inventory.

If you have Carbon Black sensors installed on your computers in addition to the Bit9 Agent, Carbon Black will continue to detect and report executions of these files.

## File Groups

**Platform Note:** For this release of the Bit9 Security Platform, only files on Windows computers are grouped by installer, so this section does not apply to other platforms.

As files are being installed on a computer, the Bit9 Agent groups them according to its analysis of what process is installing them. This group name might be unique, or it might be an installer name common to multiple groups – “setup.exe”, for example.

Once installation is complete, the agent scans the Windows program database to see whether these files can be associated with a “Programs and Features” entry. If so, files will be regrouped under the file that is used for modifying or removing corresponding programs. If no Programs and Features entry is found, installed files will retain the initial group name.

The screenshot shows the Bit9 console interface. The top window is titled "Files: All Unique Files" and displays a table of installed programs. The "Copy and Store Helper" entry is highlighted with a red box. Below this, a second window titled "Files associated with 'Copy and Store Helper'" is shown, listing five files associated with this group.

First Seen Date	First Seen Name	Product Name	Trust	Global State
Mar 29 2011 08:40:27PM	abcdegf.dll	File Copy Tool	10	Approved
Mar 29 2011 08:40:27PM	zyx.dll	File Copy Tool	10	Approved
Mar 29 2011 08:40:27PM	afile.dll	Compress File	10	Approved
Mar 29 2011 08:40:26PM	mnoqp.dll	Store This	10	Approved
Mar 29 2011 08:40:18PM	file123.exe	File Copy Tool	10	Approved

Group names are used wherever files are listed in the Bit9 Console. Examples include:

- On the File Catalog and Files on Computers pages, you can choose the Installed Programs Saved View to see a list of applications.
- In Baseline Drift Report Results, if you are looking at a Files view, you can group by Installed Program to see how much drift is attributable to each application.
- If you click on a highlighted file name in the File Catalog, you see a File Group Details page that lists all of the files associated with the file you clicked on, and usually showing the application they are part of. This is the aggregate of all unique files installed by the highlighted file, on all computers running the Bit9 Agent.
- If you click on a highlighted file name in the Files on Computers page, you see a File Group details page listing all files associated with the file instance you clicked on.

- If you click on a <Initialization files> in a row on the Files on Computers page, you see a list of all files that were present on the computer named in that row at the time the Bit9 Agent was last initialized (normally, when the agent was installed).

## Viewing Details Pages

The Bit9 Console provides two different details pages for files it manages:

- **File Details** – For *each unique file* discovered on computers running the Bit9 Agent, you can open a File Details page, which provides global information about the file and allows you to modify various global parameters for the file. The File Details page presents complete information for unique files listed in the File Catalog table.
- **File Instance Details** – For *each instance of a file* discovered on a computer running the Bit9 Agent, you can open a File Instance Details page, which provides information specific to that instance in addition to some of the global information seen on the File Details page; it also allows you to modify both instance and global attributes of the file. The File Instance Details page presents complete information for instances of files listed in the Files on Computers table.

The following sections provide an overview of file details pages, including tables of menu commands on these pages. More detailed descriptions of activities you can perform on these pages are provided elsewhere in the *Using the Bit9 Security Platform* guide, especially in [Chapter 8, “Approving and Banning Software.”](#)



## File Details Page

The File Details page shows details of the global state of a file. In any table showing unique files, such as the File Catalog, you click the View Details (pencil) button to open the File Details page.

**File Details**

**General**

- First Seen Name:** firefox.exe
- First Seen Date:** Mar 5 2015 03:35:48 PM
- Last Updated:** Mar 6 2015 08:24:18 AM
- First Seen Path:** c:\program files (x86)\mozilla firefox\updated\
- First Seen Computer:** MYCORP\Server-6
- First Seen Platform:** Windows
- Extension:** exe
- Global State:** Approved
- Global State Details:** File is approved (Reputation), Publisher is approved (Reputation), Certificate is approved
- Flags:** (none)
- Installer / Updater:** No
- Reputation Enabled:** Yes
- File Prevalence:** File exists on 6 computer(s)

[View Bit9 SRS Cloud Data](#)

**File Properties**

- Publisher:** Mozilla Corporation
- Publisher State:** Approved (Reputation)
- Certificate:** Mozilla Corporation Mozilla Corporation Mountain View CA US
- Certificate Type:** Embedded Signer
- Certificate Global State:** Approved
- Company:** Mozilla Corporation
- Product Name:** Firefox
- Product Version:** 36.0.1
- File Size:** 376,944 bytes
- Description:** Firefox
- File Type:** Application
- SHA-256:** EB38C2C5E7CC1D302D1FA6396EB3720FCAA1F91D85F22551983DF86DB8218109
- MD5:** F51D682701B303ED6CC5474CE5FA5AAA
- SHA-1:** 4D3B29D3BE1947F657C80C74DEC566C39029ADCD

**Bit9 Software Reputation Service Information**

- Trust:** 10 out of 10
- Threat Level:** 0 - Clean

**Carbon Black**

- First Seen Activity:** Mar 06 2015 11:10:25 AM
- Watchlists:** 1
- Frequency Data:** 13 computers have seen this file in 146 processes.
- Unique Paths:**

**Groups that contain this file**

- Updater.Exe** Find all files contained in this group
- Updater.Exe** Find all files contained in this group

**History**

- Mar 9 2015 10:00:40 AM** System changed the file state to "Approved (Reputation)"
- Mar 5 2015 03:35:48 PM** The file appeared on MYCORP\Server-6 post installation
- Aug 11 2012 04:09:22 PM** System changed the state of publisher Mozilla Corporation to "Approved (Reputation)"

Table 25 shows the information and actions available on the File Details page. Certain global file attributes are captured only for the “first seen” instances of the file seen by a Bit9 Agent. These are labeled as such on the File Details page.



**Table 25:** File Details and File Catalog Page Fields

Field	Description
<b>General panel</b>	
<b>First Seen Name</b>	File name of the first file to have this hash discovered by an agent managed by this Bit9 Server.
<b>First Seen Date</b>	Time the first file with this hash was seen on a network computer, displayed in the format: MM DD YYYY hh:mm:ss(AM/PM).
<b>Last Updated</b>	Last date and time when the metadata for this file was updated. (Not affected by Bit9-provided data, e.g., prevalence or trust).
<b>First Seen Path</b>	Path of the first file to have this hash reported to this server.
<b>First Seen Computer</b>	Name of the computer on which the file was first seen. Click on this name to get the Computer Details page for this computer. If you later delete the first-seen computer from the system, it is no longer associated with the file and this field is blank.
<b>First Seen Platform</b>	Platform (Windows or Mac) on which this file was first seen by this Bit9 Server.
<b>Extension</b>	File extension of the first seen file to have this hash.
<b>Global State</b>	Global State is a combination of File State and Publisher State, and indicates the overall approval state for all systems or by policy. Files can be globally approved by hash or publisher. The possible values are Approved, Banned, Unapproved, Approved by Policy, Banned by Policy, and Mixed. Global State is Mixed when a file is approved in some policies, but banned in other policies. For example, a file could be banned by hash in some policies, and approved by publisher in the remaining policies.
<b>Global State Details</b>	The File State and Publisher State contributing to Global State.
<b>Flags</b>	File-state metadata for use by Bit9 support engineers. Your support representative may ask you to report this information.
<b>Installer/Updater</b> (in File Details) <b>Installer</b> (in File Catalog)	Indicates whether either Bit9's analysis or a console user has identified this file as an installer or updater (which means that if the file is approved, so are all files that it creates). <b>Yes</b> – File is to be treated as an installer that will expand to create more files. If this file is approved, files it writes will be locally approved. <b>No</b> – File will be treated as non-expandable.
<b>Reputation Enabled</b>	Indicates whether reputation-based approval is enabled for this file (Yes or No).
<b>File Prevalence</b>	The number of computers on which this file exists. You can use the <b>Add Alert</b> command on the Actions menu to add an alert that triggers when the prevalence of a file reaches a certain level. See <a href="#">“Using Bit9 Alerts”</a> on page 494 for details.
<b>View Bit9 SRS Cloud Data</b> (button)	Click to get a detailed analysis (if available) of this file from Bit9 SRS. Button appears on the File Details page after you activate Bit9 SRS. For more information, see <a href="#">“Activating Bit9 SRS”</a> on page 643.

Field	Description
<b>File Properties panel</b>	
<b>Publisher</b>	If the file is digitally signed or was included in a digitally signed package, the console displays the publisher (software manufacturer) of the associated application.
<b>Publisher State</b>	The approval state of the publisher. Values are Approved, Approved by Policy, Banned, Banned by Policy, and Unapproved. Does not appear if the publisher is unknown.
<b>Certificate</b>	The Subject Name for the certificate that signed this file.
<b>Certificate Type</b>	For leaf certificates, certificate type indicates what the leaf certificate is being used for and how it is associated with a file. Type is some combination of the following terms: Embedded, Detached, Signer, Cosigner.
<b>Certificate Global State</b>	The effective state of the certificate. Values are Unapproved, Approved, Banned, Approved By Policy, Banned By Policy, Mixed
<b>Company</b>	The Company name (if provided) in the file metadata.
<b>Product Name</b>	The Product Name (if provided) in the file metadata.
<b>Product Version</b>	The Product Version (if provided) in the file metadata.
<b>File Size</b>	Size of the file (in bytes).
<b>Description</b>	The Description (if provided) in the file metadata.
<b>File Type</b>	<p>One of the following:</p> <p><b>Application</b> – Any executable (e.g., .exe or .com) except for Packages</p> <p><b>Supporting File</b> – Any library loaded by an executable (e.g., .dll, .ocx, .sys)</p> <p><b>Package</b> – Any installer (.exe with contents, such as a self-extracting zip or setup program)</p> <p><b>Script File</b> – Any script or batch file (e.g., .bat, .vbs, .wsf)</p> <p><b>Other</b> – Reserved for future types</p> <p><b>Unrecognized Executed File</b> – A file that was not identified as an executable by Bit9 during initialization or later analysis, but that some process attempted to execute. The execution attempt adds the file to the lists of files tracked and managed by the Bit9 Server and Agents.</p> <p><b>Unknown</b> – Files reported by older Bit9 Agents that don't provide file type information</p>

Field	Description
<b>SHA-256</b>	<p>Hash (data signature) of the file created using Bit9's proprietary SHA-256 algorithm. SHA-256 is used internally as the preferred hash for files tracked by Bit9.</p> <p>SHA-256 hashes created by the Bit9 algorithm may be identical to those created by other means. However, some files change their hash every time they are installed because they include date, location, or other context-specific information not relevant for tracking purposes. For files known to do this, Bit9 uses a special <b>fuzzy hashing</b> algorithm that eliminates this extraneous variation, and so shows every instance of such files on computers running Bit9 Agents to be identical. When this algorithm has been used, the hash is identified as "SHA-256 (Normalized)".</p> <p>You can search for files by hash using filters on the Files page or the Find Files page. <b>All File Instances</b> in the Related Views menu provides a way to do this directly from the File Details page.</p>
<b>MD5</b>	MD5 is a widely used hashing algorithm. Bit9 provides this alternate hash in case you or the system needs to identify the file against a list of published MD5 hashes.
<b>SHA-1</b>	SHA-1 is another widely used hashing algorithm. Bit9 provides this alternate hash in case you or the system needs to identify the file against a list of published SHA-1 hashes.
<b>Bit9 Software Reputation Service Information panel</b>	
<b>Trust</b>	<p>Indicates the level of trust for the file based on Bit9 Software Reputation Service (SRS) information such as file source and certificates. The trust rating is showing on a scale of 0 (none) to 10 (most trusted), along with a graphic meter reflecting this rating. Trust for a file also might be unknown, in which case this field is blank in the column for that file and shows "(unknown)" in its details page.</p> <p>The value of this field is a subjective assessment of the file's integrity. As an indication of whether the file appears to be safe based on information derived from Bit9 SRS analysis, the trust value does not signify actual approval on the Bit9 Server. However, you can use Reputation Rules to automatically approve files based on their trust rating or the trust rating of their publisher.</p>
<b>Threat level</b>	<p>If Bit9 SRS is configured, discovered files are automatically submitted for threat analysis. Bit9 SRS flags known malware with a red x icon. No flag indicates that the file was not recognized as malware, not necessarily that it is safe. Threat levels include:</p> <p><b>0</b> - Clean  <b>1</b> - Potentially malicious  <b>2</b> - Malicious  <b>Unknown</b> - Not identified</p>
<b>Category</b>	If you have configured Bit9 SRS, this shows the category this file is in (e.g., Entertainment, Hacking Tools, Instant Messaging, Media Players). Category may be unknown, and is not displayed on the details page in this case.
<b>Policy Specific States</b>	Indicates ways in which the file is treated differently in particular policies. For example, if the file is under a policy-specific hash ban or approval, the policy name is shown here. Does not appear if there is no policy specific treatment of the file.

Field	Description
<b>Carbon Black panel (all data is from Carbon Black Server)</b>	
<b>First Seen Activity</b>	The date and time when activity involving this file was first reported to the Carbon Black server.
<b>Watchlists</b>	Shows the number of Carbon Black Watchlists that this file is on.
<b>VirusTotal Score</b>	Shows the VirusTotal score for this file.
<b>Frequency Data</b>	Shows how many hosts have observed the binary with this MD5 hash value.
<b>Unique Paths</b>	Shows the number of unique paths in which this file has been seen
<b>Network Connections</b>	Shows the number of network connections that the execution of this process either attempted or established.
<b>Registry Modifications</b>	Shows the number of registry modifications made because of execution of this file.
<b>File Icon</b>	Shows the desktop icon associated with this file (if any).
<b>More information</b>	Links back to the Carbon Black console to get additional information about the file.
<b>External Analysis Results panel</b>	
<productname>	<p>If you used the Bit9 Connector to integrate the Bit9 Platform with a supported network security device or service, and you have correlated notifications from that source with the Bit9 File Catalog, files that match malicious or potential risk notifications from the third party source show those results in this panel. Possible options are:</p> <ul style="list-style-type: none"> <li>• Check Point</li> <li>• FireEye</li> <li>• Microsoft SCEP</li> <li>• Palo Alto Networks WildFire</li> </ul>
<b>Group Information panel</b>	
<group name>	If a file is the root of a group, this indicates the group name (usually the file name) and how many files are in the group. Note that tools such as browsers may appear as the root of a group because they download files. These files may appear as group members even though they are unrelated to the tool in any other way.
<b>Groups that contain this file panel</b>	
<group names>	<p>If a file is associated with a group, this panel indicates the group(s) with which this file is associated and the root file(s), if known, of the group(s). Some files may be installable by multiple root files (or be copies of another file), and so they will show multiple groups here.</p> <p>Each group shown includes a <i>Find all files contained in this group</i> link that opens the File Group Details page to show the results.</p>

Field	Description
<b>History panel</b>	
<dates and times>	<p>Indicates whether the file was identified on the first-seen computer during initialization or detected after initialization.</p> <p>Also indicates any approvals or bans applied to the file.</p> <p>Files detected <i>after</i> initialization are tracked as unapproved files until approved or banned, and may be viewed in the New Unapproved view on the Files page File Catalog tab.</p>
<b>Fields in File Catalog table only</b>	
<b>Acknowledged</b>	Indicates whether a console user acknowledged this file (Yes or No). You can acknowledge a file using the Action menu on the File Catalog tab. This can help distinguish files you already know about from new arrivals. Acknowledging a file removes it from the New Unapproved Files view but does not change its state.
<b>Approved by Reputation</b>	Indicates whether the file was approved by either its own or its publisher's reputation. (Yes or No).
<b>CL Version</b>	For individual files, the configuration list number in which the current global state for this file was defined. Agents at or beyond this CL Version have the correct global state for the file.
<b>File Size</b>	Shows the size in bytes of each file.
<b>File State</b>	<p>The approval/ban state of the file hash (Unapproved, Approved, Banned, Approved by Policy or Banned by Policy). The effective "Global State" of a file combines File State and Publisher State.</p> <p>You can change File State using the Action menu on any of the tables on the Files page or any of the details pages for files. On details pages, you can edit an existing approval or ban.</p>
<b>File State Reason</b>	For Approved or Banned file hashes, how its state was specified. The possible values are: Manual, Trusted Directory, Reputation, Imported, External (API), Unknown.
<b>Initialized</b>	Indicates whether this file was present during agent initialization (Yes or No).
<b>Installed Program</b>	<p>The full package or application name of the installed program (if any) with which this file is associated.</p> <p><b>Platform Note:</b> Only Windows files are identified as Installed Programs.</p>
<b>Marked as Installer</b>	<p>Indicates whether a file not identified by Bit9 as an installer has been marked as in installer by a console user.</p> <p><b>Yes</b> – File was marked as an installer by a user.</p> <p><b>No</b> – File was not marked as an installer by a user (although it might have been identified by Bit9 as an installer).</p>
<b>Publisher or Company</b>	The publisher (if available) or company (if available and there is no publisher information) for the file.
<b>Trusted Package</b>	<p>Indicates whether this file is part of a trusted package. (Yes or No). A trusted package is a common source or installer located in a Trusted Directory.</p> <p><b>Platform Note:</b> Only Windows files can be in a trusted package.</p>

## **File Instance Details Page**

The File Instance Details page shows information about a file instance on a computer plus some of the global file information you see on the File Details page. In any table showing file instances – for example, the Files on Computers page or Find File Results – you click the View Details (pencil) button to open the File Instance Details page.

**File Instance Details**

Details for file on computer: MYCORP\Laptop-9

<b>File Name:</b>	firefox.exe
<b>Date Created:</b>	Mar 09 2015 04:52:16 PM
<b>File Path:</b>	c:\program files (x86)\mozilla firefox\
<b>Computer:</b>	MYCORP\Laptop-9
<b>Platform:</b>	Windows
<b>User Name:</b>	(none)
<b>Local State:</b>	Approved
<b>Local State Details:</b>	Locally Approved
<b>Detached Publisher:</b>	(none)
<b>Executed:</b>	Yes
<b>Present At Initialization:</b>	No
<b>Top-Level File:</b>	No
<b>Deleted:</b>	No
<b>Root File Name:</b>	updater.exe

---

**General**

<b>First Seen Name:</b>	firefox.exe
<b>First Seen Date:</b>	Mar 5 2015 03:35:48 PM
<b>Last Updated:</b>	Mar 6 2015 08:24:18 AM
<b>First Seen Path:</b>	c:\program files (x86)\mozilla firefox\updated\
<b>First Seen Computer:</b>	MYCORP\Server-6
<b>First Seen Platform:</b>	Windows
<b>Extension:</b>	exe
<b>Global State:</b>	Approved
<b>Global State Details:</b>	File is approved (Reputation), Publisher is approved (Reputation), Certificate is approved (none)
<b>Flags:</b>	(none)
<b>Installer / Updater:</b>	No
<b>Reputation Enabled:</b>	Yes
<b>File Prevalence:</b>	File exists on 6 computer(s)

[View Bit9 SRS Cloud Data](#)



---

**File Properties**

<b>Publisher:</b>	Mozilla Corporation
<b>Publisher State:</b>	Approved (Reputation)
<b>Certificate:</b>	Mozilla Corporation Mozilla Corporation Mountain View CA US
<b>Certificate Type:</b>	Embedded Signer
<b>Certificate Global State:</b>	Approved
<b>Company:</b>	Mozilla Corporation
<b>Product Name:</b>	Firefox
<b>Product Version:</b>	36.0.1
<b>File Size:</b>	376,944 bytes
<b>Description:</b>	Firefox
<b>File Type:</b>	Application
<b>SHA-256:</b>	EB38C2C5E7CC1D302D1FA6396EB3720FCAA1F91D85F22551983DF86D88218109
<b>MD5:</b>	F51D682701B303ED6CC5474CE5FA5AAA
<b>SHA-1:</b>	4D3829D3BE1947F657C80C74DEC566C39029ADCD

---

**Bit9 Software Reputation Service Information**

<b>Trust:</b>	 10 out of 10
<b>Threat Level:</b>	 0 - Clean

---

**Carbon Black**

<b>First Seen Activity:</b>	Mar 06 2015 11:10:25 AM
<b>Watchlists:</b>	1
<b>Frequency Data:</b>	8 computers have seen this file in 96 processes.
<b>Unique Paths:</b>	

---

**Groups that contain this file**

<b>Updater.Exe</b>	Find all files contained in this group
<b>Updater.Exe</b>	Find all files contained in this group

---

**History**

<b>Mar 9 2015 10:00:40 AM</b>	System changed the file state to "Approved (Reputation)"
<b>Mar 5 2015 03:35:48 PM</b>	The file appeared on MYCORP\Server-6 post installation
<b>Aug 11 2012 04:09:22 PM</b>	System changed the state of publisher Mozilla Corporation to "Approved (Reputation)"

Many File Instance Details fields are identical to those on the File Details page (Table 25) and you can take many of the same actions from the File Instance Details page. Table 26 shows the additional fields available on the File Instance Details page and Files on Computers table. On the details page, these appear in the top panel, which is labeled **Details for file on computer:** <computername>.

**Table 26:** Additional Fields: File Instance Details and Files on Computers

Field	Description
<b>File Instance Details: File on computer panel</b>	
<b>File Name</b>	File name of this instance.
<b>Date Created</b>	Exact time this instance was created in its current location, displayed in the following format: MM DD YYYY hh:mm:ss(AM/PM).
<b>File Path</b>	Path of the this file instance.
<b>Computer</b>	Name of the computer this instance is on.
<b>Platform</b>	Platform (Windows, Mac) of the system the instance is on.
<b>User Name</b>	Name of the user logged in when this file was created.
<b>Local State</b>	The local state of the file instance (Unapproved, Approved, Banned, Deleted). If the local state is Unapproved, you can choose <b>Approve Locally</b> on the Actions menu. If it is Approved, you can <b>Remove Local Approval</b> . If it is Banned, you cannot change it.
<b>Local State Details</b>	File-state metadata for use by Bit9 support engineers. If necessary, your support representative may ask you to report this information. See Table 32 for details.
<b>Detached Publisher</b>	If this file did not have its own certificate but was indirectly signed via a “detached certificate,” this field appears and shows the name of the publisher. Some publishers distribute updates as collections of unsigned files with a <i>catalog</i> that contains hashes of all indirectly signed files and is itself signed. Bit9 can use these catalogs to verify publishers and allow publisher-based approval of files signed in this way.
<b>Detached Publisher State</b>	(If there is a detached publisher) These options are the same as for Publisher State: Approved, Approved by Policy, Banned, Banned by Policy, Unapproved.
<b>Executed</b>	Indicates whether this file instance has been executed or not.
<b>Present at Initialization</b>	Indicates whether this file instance was among the files present on the computer when the Bit9 Agent was installed, or whether it appeared after installation.
<b>Top-Level File</b>	Indicates whether the file is a top-level file; that is, one that was not installed by or copied from another file. <b>Platform Note:</b> On Windows systems, files that were discovered during initialization can be later assigned top-level status if they are discovered to be installers.



Field	Description
<b>Deleted</b>	Indicates whether this file instance has been deleted from the computer it was on. This is a temporary state immediately after file deletion and before it is removed from the database for this Bit9 Server.
<b>Root File Name</b>	File that wrote the current file. If this is a top-level file, there is no root file and the name is <i>(none)</i> .
<b>Fields in Files on Computer table only</b>	
<b>Computer Tag</b>	For the computer on which the file appears, displays the optional Computer Tag if provided.
<b>IP Address</b>	The IP address of the computer on which the file appears.
<b>Operating System</b>	The operating system of the computer on which the file appears.
<b>Policy</b>	The Bit9 security policy of the computer on which the file appears.

## Menus on the Files Pages

### Menus on the File Details Page

The File Details page includes three menus to the right of the file information: a Related Views menu, an Actions menu, and an Advanced menu. The File Catalog and Files on Computers tabs have an Action menu in the upper left above the table. [Table 27, “Menus on File Tables and Details Pages,”](#) shows the available choices on file page menus. Note that some choices are available only for certain file states.

### Menus on the File Instance Details Page

The File Instance Details page includes three menus to the right of the file information: a Related Views menu, an Actions menu, and an Advanced menu. It is similar to the File Details page menu, except that includes options for local approval. [Table 27, “Menus on File Tables and Details Pages,”](#) shows the available choices on file page menus.

#### Notes

- Some menu choices are available only for certain file states.
- Many of these commands are also available on the Events page Action menu when the view includes file-related events.

**Table 27:** Menus on File Tables and Details Pages

Menu Choice	File Catalog	Files on Computers	File Details	File Instance Details
<b>Related Views menu</b>				
All File Instances			X	X
File Events			X	X
Carbon Black Details			X	X
Computers with this file			X	X
Computers without this file			X	X
<b>Actions menu</b>				
Approve Locally		X	X	X
Remove Local Approval		X		X
Approve Globally	X	X	X	X
Ban Globally	X	X	X	X
Approve by Policy	X	X	X	X
Ban by Policy	X	X	X	X
Edit Global Approval/Ban Edit Approval/Ban by Policy			X	X
Remove Approval or Ban	X	X	X	X
Acknowledge	X			
Find computers with at least one of the selected files			X	X
Find computers with all of the selected files			X	X
Find computers missing at least one of the selected files			X	X
Find computers missing all of the selected files			X	X
Add/Edit Meter			X	X
Add/Edit Alert			X	X
<b>Advanced menu</b>				
View Bit9 SRS Data	X	X	X	X
Enable/Disable Reputation for this File			X	X
Mark as Installer/Not Installer			X	X
<b>External Pages menu</b>				
File Analytics			X	X

## Summary of File Views

The previous sections provided details of the main views of file information in the Bit9 Console. [Table 28](#) summarizes how to “drill down” for access to particular views of this information.

**Table 28:** File Views and File Details in the Bit9 Console

To view...	...do this
A table of all unique <i>top-level</i> files (files not installed by another file) discovered on computers managed by your Bit9 Server.	<p>Go to <b>Assets &gt; Files</b>, click on the <b>File Catalog</b> tab, and make sure the <i>Show individual files</i> box is <i>not</i> checked.</p> <p><b>Notes:</b> Top-level files are files that do not have an associated installer, or whose installer is unknown. If a top-level file <i>is</i> an installer, its name shows as a highlighted link to its associated files.</p>
A table of all unique individual files discovered on computers managed by your Bit9 Server.	<p>Click on the <b>File Catalog</b> tab, and check the <i>Show individual files</i> box.</p> <p><b>Notes:</b> This view shows both files installed by other files and top-level files. Names of known installers are highlighted.</p> <p><b>Important:</b> There can be millions of unique files discovered by the Bit9 Server, and this view can cause performance issues on underpowered servers.</p>
The global file details for one unique file.	<p>Click on the <b>File Catalog</b> tab, and click the View Details button next to the file for which you want details.</p>
A table of all files on all computers managed by your Bit9 Server that are associated with (usually meaning installed by) one top-level file:	<p>Click on the <b>File Catalog</b> tab, make sure the <i>Show individual files</i> box is not checked, then click the name of the file for which you want a list of associated files.</p> <p><b>Notes:</b> This is an aggregate list of associated files, not based on installations seen on one particular computer. For example, if installer X was seen installing files A and B on one computer and installing files B and C on another computer, all installed files (A, B and C) would be listed in the File Group Details page of installer X. For details on any file in the table, click the View Details button next to it.</p> <p><b>Platform Note:</b> In this Bit9 release, only files on Windows computers are grouped by installer.</p>

To view...	...do this
<p>A table of all <i>top-level</i> file instances (not installed by another file) on all computers managed by your Bit9 Server:</p>	<p>Click on the <b>Files on Computers</b> tab, and make sure the <i>Show individual files</i> box is <i>not</i> checked.</p> <hr/> <p><b>Notes:</b> Top-level files are files that do not have an associated installer, or whose installer is unknown. If a top-level file <i>is</i> an installer, its name shows as a highlighted link to its associated files.</p> <p>This table view also includes an entry named &lt;Initialization files&gt; for each agent, which is a grouping of the files found on the computer at the time the agent was installed.</p>
<p>A table of all file instances found on one computer at <i>initialization</i>, which occurs either when the agent is initially installed or when a disabled agent is re-enabled:</p>	<p>Click on the <b>Files on Computers</b> tab, and make sure the <i>Show individual files</i> box is <i>not</i> checked. Then click on &lt;Initialized files&gt; in the row containing the name of the computer you are interested in.</p>
<p>A table of <i>all</i> individual file instances on all computers managed by your Bit9 Server:</p>	<p>Click on the <b>Files on Computers</b> tab, and check the <i>Show individual files</i> box.</p> <hr/> <p><b>Notes:</b> This view shows both top-level and “individual” files that were installed by them on an agent-managed computer. Top-level files that have been analyzed by the agent to determine their contents show as highlighted links.</p> <p><b>Important:</b> Avoid checking this box unnecessarily, especially if you have a large number of agent-managed computers. The total number of individual files could number in the tens or hundreds of millions. Attempting to load a list of this many files can cause the Bit9 Server to time out.</p>
<p>The details for one file instance on one computer.</p>	<p>Click on the <b>Files on Computers</b> tab, and click on the View Details button next to the file instance for which you want details.</p> <hr/> <p><b>Notes:</b> Opens the File Instance Details page. Shows both local state and other information about this instance and global details for the file. Top-level files can still appear in Files on Computers tables after they are no longer present. Clicking View Details for a removed file no longer present on a computer will show global details only.</p>
<p>A table of all files on one computer that are associated with one top-level file:</p>	<p>Click on the <b>Files on Computers</b> tab, and click on the name of the highlighted top-level file instance for which you want a list of associated files.</p> <hr/> <p><b>Notes:</b> Shows the results of a Find Files search for all files on <i>the named computer</i> in the row that are associated with the file whose name you clicked on.</p> <p>For details on any file in the table, click the View Details button next to it.</p>

## Global File State

Files in the File Catalog tab on the Files page have the following high-level states:

- **File State** indicates the approval/ban state of the file itself.
- **Publisher State** is the approval state of the file's publisher (if known). The only choices are Approved, Approved by Policy, and Unapproved.
- **Global State** combines File State and Publisher State to determine how the file is to be treated on agent-managed computers. The File State and Global State are the same except when:
  - Publisher State is *not* Unapproved, *and*
  - File State is *not* approved or banned in the same policies as the publisher.

Global State cannot be modified directly. [Table 29](#) shows the possible Global States.

**Table 29:** Global State (for files) cataloged by a Bit9 Server

State	Description
<b>Approved</b>	Allowed to execute on all computers.
<b>Banned</b>	Banned by hash, and not allowed to execute on any computer running in Control mode.
<b>Approved by Policy</b>	Allowed to execute on computers in one or more policies.
<b>Banned by Policy</b>	Banned by hash from execution on computers in one or more policies (in Control mode).
<b>Unapproved</b>	Not Approved or Banned (globally or by policy). Bit9 blocks or permits execution of an unapproved file based on the Enforcement Level of the Policy of the computer attempting the execution.
<b>Mixed</b>	Effective state varies by policy because File State is Banned for some policies but the Publisher State is Approved for some or all policies.

## Flags

Global State is the effective Bit9 classification of each unique file in the File Catalog. It is a combination of the File State and the Publisher State for the file. *Flags* are primarily for use by Bit9 Technical Support, but you might find them useful in determining how a file is being labeled or handled in your Bit9 environment.

**Table 30:** File Flags

Flag	Description
<b>Report Only Ban</b>	File was identified by a Bit9 Console user so that attempts to execute it are reported as if they would have been banned, but it is not blocked from execution.
<b>Installer</b>	File was identified as an installer by Bit9 and is allowed to execute. If executable files are written out by it, they are locally approved. <b>Platform Note:</b> For this Bit9 release, on Mac computers, only files associated with the native Mac updater (i.e., .pkg files) are identified as installers.
<b>Installer (Override)</b>	File was identified as <i>not</i> being an installer by Bit9, but a Bit9 Console user changed it to “installer”. If it is allowed to execute, the executable files it writes out are locally approved.
<b>Not installer (Override)</b>	File was identified as an <i>installer</i> by Bit9, but a Bit9 Console account user changed its installer status to “Not installer”.

## Local File State

Files that are globally Banned or Approved have the same local and global state. Files with a Global State of Unapproved may have different Local States. In particular, it is possible to locally approve a file by a variety of methods, as long as that file was not globally banned. You can view local file state on the Files on Computers tab of the Files page.

**Table 31:** Local State

State	Description
<b>Approved</b>	This instance of the file is approved for execution. Local approval can be due to approval by name or hash for all computers in a policy or all computers managed by this Bit9 Server. It also could be due to a global approval method, a change in Enforcement Level, or an explicit Local Approval of this single file instance. Locally approved files can have a <i>global state</i> of Unapproved or Approved, but not Banned.
<b>Banned</b>	This instance of the file is banned from execution. A file that has a local state of banned might be banned on all computers in certain policies or all computers managed by this Bit9 Server. Note that banning a file by name does not change its local state.
<b>Unapproved</b>	This instance of the file has not been approved or banned. Its execution is blocked or permitted based on the Enforcement Level of the computer it is on.
<b>Deleted</b>	This instance of the file has been deleted, but the record of it still exists in the database for this Bit9 Server.

## Local State Details

Local State is the Bit9 classification of a particular instance of a file on a particular computer. This information is primarily for use by Bit9 Technical Support, but you might find it useful in determining why a file was assigned its top-level Local State.

**Table 32:** Local (File) State Details

State	Description
<b>Approved</b>	Approval state on the local computer for files that are globally approved in the File Catalog.
<b>Approved (Not Persisted)</b>	Approval state on the local computer for files that were approved by certain pre-version-6.0 methods but are not globally approved in the File Catalog. If you delete a file in this state, new instances would not necessarily be locally approved.
<b>Approved as Installer</b>	Approval state for top-level installers (in Windows) that indicates that the installer and the files it contains have been hashed, analyzed, and globally approved by Bit9. When users execute these files, the Bit9 Agent permits them to run as globally approved files. This state is not common and unnecessary for local approval of files generated by an installer.
<b>Approved as Installer (Top Level)</b>	Approval state for top-level installers. The installer has been globally approved and when executed, the files it generates are locally approved. <b>Platform Note:</b> For this Bit9 release, on Mac computers, only files associated with the native Mac updater (i.e., .pkg files) are identified as installers.
<b>Banned</b>	Files with specified hash are not allowed to execute on the computers specified (all computers or by policy).
<b>Banned (Report Only)</b>	Test file state for files that are to be banned by hash. Bit9 permits files that are banned but in Report-Only to execute but records a “would have blocked” message in the event log to show how the file would have been handled if the ban were active.
<b>Locally Approved</b>	File is approved to run on the local computer but unapproved (globally or for the current policy) in the File Catalog. Files can be locally approved so that they can be installed on one computer without approving them for any other computer running the Bit9 Agent.
<b>Locally Approved (Auto)</b>	File is approved to run on the local computer because it was written by a trusted installer or updater. Other than the source of its approval, this is the same as Locally Approved.

State	Description
<b>Unapproved</b>	File appeared after agent initialization and has not been approved. Depending on Enforcement Level on each computer, the agent either blocks the file or permits its execution. These files might become locally approved if a computer transitions from Low (or no) Enforcement to Medium or High, depending upon policy settings. Files are assigned Unapproved local state details if the first local instance was found when the Enforcement Level was Low (Monitor Unapproved) or None (Visibility Only). See <a href="#">“Automatic Local Approval on Enforcement Level Change”</a> on page 253 for details of this behavior.
<b>Unapproved (Persisted)</b>	File appeared after agent initialization and has not been approved. Unapproved (Persisted) files do not become locally approved when a computer changes from Low or None (Visibility) Enforcement to High or Medium Enforcement. Files are assigned Unapproved (Persisted) local state details if the first local instance was found when the machine was in High or Medium Enforcement Level.

## Publisher Information

The Publishers tab on the Software Rules page shows file publishers discovered on computers running the Bit9 Agent in your organization. It also shows any publishers that have been added manually to the File Catalog for your Bit9 Server. This page includes an Action menu that allows you to approve or ban a publisher, remove approvals or bans, and acknowledge a publisher to indicate that you have reviewed it already. These actions are described in [“Approving or Banning by Publisher”](#) on page 236.

**To view the list of discovered or added publishers:**

1. On the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click the **Publishers** tab. All publishers of signed software installed on agent-managed computers reporting to your server, plus any publishers you manually added using certificates, appear in the Publishers table:

Name	Date Approved	Approved By	Trust	State Reason
State: Approved 22 items				
Adobe Systems Incorporated	Nov 29 2011 09:53:09AM	rjones@mycorp.local	High	Manual
Adobe Systems, Incorporated	Nov 29 2011 09:53:13AM	rjones@mycorp.local	High	Manual
Bit9, Inc	Jun 01 2010 11:45:59AM	System	High	Manual
Bit9, Inc	Jun 01 2010 11:45:59AM	System	High	Manual
Dell Inc	May 09 2007 07:22:06AM	dgomez@mycorp.local	High	Manual
Dell Inc.	May 09 2007 07:22:18AM	dgomez@mycorp.local	High	Manual



You can view a Publisher Details page for any publisher shown in the Publishers table by clicking on the View Details (pencil and file) button next to the publisher name. In addition to details (see Table 33), the Publisher Details page has shortcuts with which you can Approve or Remove Approval for the publisher. The Related Views menu also includes a command that shows all files from the publisher as well as commands that show computers where the approval state for this publisher is up-to-date.

**To view complete details for one publisher:**

1. On the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click the **Publishers** tab. All publishers of signed software installed on agent-managed computers on your network appear in the Publishers table.
3. From the table of publishers, locate the publisher you want to authorize and click on the View Details button (pencil and file). The Publisher Details page opens.

**Publisher Details**

**General**

**Publisher Name:** VMware, Inc.  
**State:**   Enable reputation approvals for this publisher  
**Acknowledged:**   
**Trust:** High  
**Description:**   
**Rule Applies To:**  All policies  Selected policies  
**Platforms:**  All platforms  Selected platforms

▶ All Certificates For This Publisher (click to expand)

**History**

<b>Date First Seen:</b>	Apr 4 2014 01:30:20 PM
<b>Platform First Seen:</b>	Windows
<b>Computer First Seen:</b>	MYCORP\DESKTOP-8
<b>Date Approved:</b>	Apr 16 2014 02:10:21 PM
<b>Approved By:</b>	admin
<b>CL Version:</b>	752

**Related Views**

- All files signed by this publisher
- All Computers that have received this rule
- All Computers that have not yet received this rule

**Table 33: Publisher Details**

Field	Description
<b>General panel</b>	
<b>Publisher Name</b>	The name of this publisher as it appears in its certificate.
<b>State</b>	Approved, Unapproved, or Banned.
<b>Enable reputation approvals...</b>	This checkbox appears if you have reputation approvals enabled. <i>Enable reputation approvals for this publisher</i> is checked by default and allows this publisher to be approved by reputation. Removing the check disables reputation approvals for this publisher, but if reputation approvals were already globally enabled, removal only affects files first seen after the change.
<b>Acknowledged</b>	You can Acknowledge a publisher, which indicates that you have reviewed it. This can help distinguish new publishers from those you already know about.
<b>Trust</b>	This field appears if you have Bit9 SRS enabled. Shows the trust rating for this publisher, which can be High, Medium, Low, or Not Trusted.
<b>Description</b>	Optional additional description of this publisher and its state.
<b>Rule Applies To</b>	For publishers that do not have reputation approval enabled, you can apply the publisher state to computers in all policies or only to those in some policies.
<b>Approved Platforms</b>	You can apply the publisher state to computers in all platforms or choose a specific platform (Windows, Mac). <b>Platform Note:</b> Publisher approvals work on Windows only.
<b>Date First Seen</b>	When this publisher was first seen on a agent-managed computer reporting to your server.
<b>History panel</b>	
<b>Platform First Seen</b>	The platform (Mac or Windows) of the computer on which this publisher was first reported to your server.
<b>Computer First Seen</b>	The computer on which this publisher was first reported to your server.
<b>Date Approved</b>	If the publisher is approved, when that approval was made.
<b>Approved By</b>	The Bit9 Console user who approved the publisher. Publishers approved by reputation may show "System" in this field.
<b>Date Acknowledged</b>	If the publisher has been acknowledged, when it was acknowledged.
<b>Acknowledged by</b>	If the publisher has been acknowledged, the Bit9 Console user that acknowledged this publisher.
<b>CL Version</b>	The version of the Bit9 Platform rules containing current publisher state. This helps determine whether an agent has the rule.

## Chapter 8

# Approving and Banning Software

This chapter describes how to approve or ban software using the Bit9 Security Platform. It includes information about both global and local file approval. Many of the methods for approving and banning software are found on one of the tabs of the Software Rules pages.

In addition to explicit approvals and bans, the Bit9 Security Platform allows you to define Custom Rules for allowing or blocking file execution or writing at specified locations, and if you choose, by specified users and/or processes. See [Chapter 12, “Custom Software Rules.”](#)

### Sections

Topic	Page
<a href="#">What is Bit9 Software Approval?</a>	224
<a href="#">What are Bit9 Software Bans?</a>	226
<a href="#">Approving by Trusted Directory</a>	228
<a href="#">Approving by Trusted User or Group</a>	234
<a href="#">Approving or Banning by Publisher</a>	236
<a href="#">Approving by Updater</a>	246
<a href="#">Locally Approving Files</a>	252
<a href="#">File-Specific Rules: Approvals and Bans</a>	266
<a href="#">Approving or Banning Lists of Files</a>	277
<a href="#">Enabling Bans to Stop Running Processes</a>	279

## What is Bit9 Software Approval?

Software approval ensures that users of computers running the Bit9 Agent can freely install and run *known-good* applications regardless of the Bit9 security settings and Enforcement Level in effect. The Bit9 Security Platform supports several complementary methods for approving software on computers. Based on the method(s) you select, installation of approved software may be permitted on all computers, on computers in selected policies, or on individually selected computers.

You can choose the combination of methods that best conforms to your established settings and procedures, especially the software distribution process in place at your site:

- When you need to pre-approve applications to run on all computers (or all computers in selected policies), designate trusted directories, approve specified publishers to allow installation of their applications, or enable certain updaters to update applications automatically.
- When you would like to pre-approve low-threat applications to run on all computers (or all computers in selected policies), enable reputation rules based on the trust level reported by Bit9 SRS for specific files and publishers.
- When you discover an individual file or installer that you want to allow to run on all computers or all computers in selected policies, create a File Approval rule.
- When you have a list of hashes for files you want to approve, you can create approvals for the entire list in a single operation.
- When you need to approve software for installation on selected individual computers, either designate trusted users (or groups) to perform installations, or choose a local approval method.
- When you have a special need for a rule to allow installation or execution of files in particular locations, or by particular users or processes, create a Custom Rule.

### Tip

At all Enforcement Levels except for High, users can install unapproved software. Although not required, Bit9 recommends approving (or at least Acknowledging) widely used software even if you plan to run at Low Enforcement Level. Approval reduces the number of files with the unapproved status, which can enable you to focus on files that are of potential concern. For example, approving known-good files generally reduces the size and increases the readability of Baseline Drift reports.

Similarly, computers operating in Visibility mode can run *any* software, regardless of its approval state. Even if you are running all your computers in Visibility mode, you might want to approve known-good files to reduce the amount of event data collected about those files. This also helps prepare you for possible transition of some or all computers into High or Medium Enforcement Level in the future.

Based on your internal standards and procedures, and on the required scope of the approval (network-wide or computer-specific), you can choose to approve files in any of the ways shown in [Table 34](#).

**Table 34:** Bit9 File Approval Methods

Approval Method	Software Is Approved for	When to Use
<a href="#">Approving by Trusted Directory</a>	All computers (global)	When you have a trusted, secure server (e.g., for software deployment) on which to create an authorized approval directory.
<a href="#">Approving by Trusted User or Group</a>	Installation computer only (local)	When you want to give unlimited installation privileges to a Windows user account or all users in a Windows or AD group. Trusted users are allowed to install on any computer on which they log in with their credentials.
<a href="#">Approving or Banning by Publisher</a>	Installation computer only (local), but can be installed on demand by any computer	When you want to approve all software from a vendor for which Bit9 can confirm a valid digital certificate. You also can approve or ban certificates that identify a publisher, and this affects file state. See <a href="#">“Using Certificates for Enforcement”</a> on page 304.
<a href="#">Approving by Publisher Reputation (see Chapter 9, “Reputation Approval Rules”)</a>	Installation computer only (local), but can be installed on demand on any computer	When you want to automatically approve all software from all publishers considered trustworthy by Bit9 Software Reputation Service (SRS).
<a href="#">Approving by Updater</a>	Installation computer only (local), but can be installed on demand on any computer	When you want to permit installation of application updates as they become available for download via specified application update programs.
<a href="#">Automatic Local Approval on Enforcement Level Change</a>	Installation computer only (local)	When you want to locally approve <i>unapproved files found while in Low enforcement or higher</i> when you move the computer from a less secure Enforcement Level to either Medium or High.
<a href="#">Moving Computers to Local Approval Mode</a>	Installation computer only (local)	When you want to permit users on computers in High Enforcement policies to install software. Local approval occurs when a user installs an unapproved file while in this mode.
<a href="#">Locally Approving All Unapproved Files on a Computer</a>	Installation computer only (local)	When you want to locally approve all existing unapproved files on a specific computer.
<a href="#">Locally Approving Individual Files</a>	Installation computer only (local)	When you want to select specific files on a computer for local approval. You can locally approve files, or remove local approval.
<a href="#">File Approval Rule</a>	Approved for all computers or those in selected policies	When you want to ensure that a known-good application can run on any computer, approve it by hash.
<a href="#">Approving by File Reputation (see Chapter 9, “Reputation Approval Rules”)</a>	Approved for all computers or those in selected policies	When you want to automatically approve (by hash) all software that Bit9 SRS considers trustworthy.
<a href="#">Approving by Event Rule (see Chapter 16, “Event Rules”)</a>	Varies by rule	When you want to automatically approve a file, either locally or globally, when it is included in a reported event.

## Platform Considerations for Rule Specifications

Many Bit9 Security Platform rules involve specification of a file name and/or path, or other manually entered information such as a user, group, or computer name. On both Mac and Windows computers, file names, paths, and user names in rules normally are *not* case sensitive. On Linux computers, file and user names in rules normally *are* case sensitive; for example, if you create a rule to ban `/temp/myfile.exe`, it will not block the files `MyFile.exe` or `/TEMP/myfile.exe`. There are two additional factors to consider in determining how case sensitivity works for rule parameters:

- Regardless of the general case-sensitivity rule for an operating system, it is actually the file system that determines case sensitivity. If a case-sensitive file system is attached to a computer whose standard file system is not case-sensitive, Bit9 rules will be case sensitive, and vice versa. Keep this in mind when you connect an external drive or mount a network file system to a Bit9-managed computer.
- The case of text entered in rule fields is preserved even if it is not relevant in its current use. This might be significant if you copy information to a place in which it applies to a different platform.

When you enter a path, be sure to use the correct directory delimiters for the platform it applies to, and to use only characters and formats legal for paths in the chosen platform. The Bit9 Server does not convert paths between platforms (e.g., `\` to `/`), although it will display a warning in some cases if the delimiter is known to be a mismatch for the platform.

## What are Bit9 Software Bans?

Bit9 file bans are rules that block specific files from executing on computers running the Bit9 Agent, based on the agent Enforcement Level (see [Table 35](#)). You can ban files reported by your Bit9 Agents in the course of day-to-day operations, and you also can preemptively ban files not yet seen on your computers but for which you have obtained information from third-party sources. Bit9 supports bans by file name or hash. Bans can affect all agents running in Control mode or be targeted to computers in selected policies only. You also can configure Bit9 to terminate processes already running when you ban their file image.

As the table shows, file bans do not prevent software from running on computers operating in Visibility mode. However, even in Visibility, a ban will produce an event that you can use to monitor how often the banned file is run. Banning undesirable files while in Visibility mode also helps you prepare for a transition into full Control mode in the future.

**Table 35:** How File Bans affect File Execution, by Enforcement Level

Policy Settings	Enforcement Levels				
	None (Agent Disabled)	None (Visibility Only)	Low	Medium	High
Banned files (by hash or name)	Off/Permit	Permit & Report	Block	Block	Block

When you ban specific files by name or hash, the bans appear as rules on the Software Rules page Files tab.

One fundamental decision about how you ban a file is whether you ban it by name or by hash. [Table 36](#) describes the differences between the two.

**Table 36:** Name vs. Hash Bans

Ban Type	Description
<b>File Name Ban</b>	<p>Block execution of the named file everywhere (if you enter only the file name) or at specified locations (if you enter a path), and on all computers or computers in selected policies. File name bans do not change the Global State of a file, but assure that all instances of files by the specified name are locally banned wherever they appear.</p> <p>Be careful not to ban a file required for system or application operation, especially when you specify paths using the (*) wildcard character.</p> <p>As a precaution, you can execute file-name bans in Report-Only state to test the effects of the ban. Ban (Report Only) bans remain unenforced until you change them to a blocking Ban.</p> <p>When you search by state for a file that is banned by both name and by hash, the file appears in the list of files in the Banned state but not in files with Local State Details of Banned by Name.</p> <p><b>Platform Note:</b> Each file name ban is specific to one platform only. If you enter a path, be sure to use the correct directory delimiters, and to use only characters and formats legal for paths in the chosen platform.</p>
<b>Hash Ban</b>	<p>Block execution of the specified hash in any location on all computers or on computers in selected policies. Hash bans are not platform-specific.</p> <p>Although you can copy and paste hashes from external sources, it is easier to ban hashes discovered by an agent directly from console pages that list files. You can create a Ban directly from most console pages that show a hash. Bans initiated from these pages automatically direct you to the Add File Rule page, fill in the hash for you, set the Type as <i>Ban</i>, and allow you to modify other ban properties before creating the ban.</p>

## File Ban Options

In addition to bans applied directly to specific files to prevent future execution, Bit9 provides many other methods and options. The following list summarizes options for banning software:

- When you want to prevent certain software from running on all computers or all computers in selected policies, create a File Ban rule for each file, which blocks it on all computers running in Control mode (or if you are running in High Enforcement, simply do not approve it). See [“File-Specific Rules: Approvals and Bans”](#) on page 266 for details on how to create these bans.
- When you have a list of hashes for unwanted files you want to ban, you can create bans for the entire list in a single operation. See [“Approving or Banning Lists of Files”](#) on page 277 for details on how to create these bans.



- When you want to ban all files from a particular publisher, ban the publisher. See [“Approving or Banning by Publisher”](#) on page 236 for more details. You can further fine-tune publisher bans by banning a specific certificate from a publisher. See [“Using Certificates for Enforcement”](#) on page 304 for more details.
- When you have a special need for a rule to block or allow installation or execution of files in particular locations, or by particular users or processes, create a Custom Rule that blocks execution – this is not a ban but can act like a ban when conditions match its criteria. See [Chapter 12, “Custom Software Rules,”](#) for more details.
- When you want to ban currently running processes with banned images in addition to future attempts to execute a file, configure Policies to do so. See [“Enabling Bans to Stop Running Processes”](#) on page 279 for more details.
- When you want to ban files when they are referenced in certain events, including malware reports from external notifications, create an Event Rule. See [Chapter 16, “Event Rules,”](#) for more details.

## Approving by Trusted Directory

If your organization uses software deployment tools, or if you want to dedicate a computer for software approval, you can use a trusted directory to automatically approve software during regular roll-outs. Trusted directory approval easily integrates with existing software deployment processes. All software in the specified trusted directory of your deployment server is automatically approved. The level of approval provided by a trusted directory depends upon the platform on which it is located.

Bit9 has tested and fully supports trusted directory approval with common deployment technologies. Please contact Bit9 Technical Support to determine whether your deployment method is supported and for guidance on any special considerations for integrating it with the Bit9 Security Platform.

Trusted Directory approvals are not sent to agents immediately upon activation of the directory or addition of files to it. There are three conditions that cause a trusted directory file approval to be sent to endpoints:

- If the Bit9 Server has a record of a file being blocked *on any endpoint* and that file is later approved by trusted directory, the server begins sending the approvals of the file to agents immediately.
- If a user attempts to execute an instance of a trusted-directory-approved file on a computer connected to the Bit9 Server, the server will allow the agent to run the file immediately, and also will begin sending the approval to other agents.
- If the trusted-directory-approved file is identified as an installer, the Bit9 Server begins sending the approval of the file to agents immediately.

Even if a file is approved by trusted directory and not blocked by another rule, until its approval is sent to agents because of one of the cases above, instances of the file may be locally unapproved and may block if the agent computer is disconnected from the server before the approval is distributed.



**Note**

Removable media should not be used for trusted directories. If a removable device is disconnected and then reconnected, it is not rescanned, and so any new content is unprocessed and untrusted. You would have to disable and re-enable the trusted directory to trust the new content. Configure trusted directories on permanently attached fixed media so that the agent can monitor modifications and additions, and can process any new content.

**Windows Trusted Directories**

On Windows computers, files found in a trusted directory (and any of its subfolders) are themselves approved.

**Archives and Installers in Trusted Directories**

Archives and installers are file types that can generate other files. It can be convenient to put both types of files in a trusted directory to make file approvals more efficient, but note that they are treated differently:

- **Archives** – Bit9 recognizes the following Windows formats as *archives*: 7Zip, BZip2, CAB, GZip, ISCab, ISO, MSCompress, RAR, ZIP and TAR.

In a trusted directory, archive files are analyzed by Bit9 to determine what files they will write when expanded. The files that will be written by the archive file are globally approved and added to the File Catalog, even if there are no instances of them yet. They are not, however added to the Files on Computers inventory until the archive is expanded on some computer. The top-level archive file (e.g., myfiles.ZIP) is not added to the File Catalog.

- **Installers** – Bit9 recognizes these common Windows formats as *installers*: NullSoft, Wise, InstallShield, and MSI. You also can manually mark files as installers.

In a trusted directory, an installer file is globally approved and added to the File Catalog. If the system hosting the trusted directory is running an agent, the installer is also added to the Files on Computers list. Installer files are *not* analyzed to determine the files they *will write* when run, nor are the files an installer will write added to the File Catalog or Files on Computers list until the installer is actually run. Instances of files written by an installer are locally approved; these files are not globally approved in the File Catalog.

**Mac and Linux Trusted Directories**

On Mac and Linux computers, top-level files found in a trusted directory (and any of its subfolders) are approved, but their contents are not analyzed or approved. For example, files that an installer *would* install or files that *could be* extracted from an archive file are neither analyzed nor approved when their top-level file is placed in a trusted directory.

However, on Mac computers, if a PKG file is placed in a trusted directory, it becomes an approved *installer*. This means that even though the PKG file was not analyzed, anything written from the PKG by the installer process will be approved.

For both Mac and Linux trusted directories, you can accomplish global approval of the files for an application or archive by expanding or extracting the package so that the files it would install or extract are actually in the trusted directory.

## Creating a Trusted Directory

Trusted directories must be on a computer with the Bit9 Agent installed. From the Bit9 Console, you specify the deployment server name and the directory to trust on that server.

### To use a trusted directory to automatically approve software for deployment:

1. If you haven't already done so, install the Bit9 Agent on the deployment server. Wait for the server's files to complete initialization. You can monitor initialization status of the deployment server on the Computers or Computer Details page (see [“Viewing Complete Details for One Computer”](#) on page 132).
2. On the console menu, choose **Rules > Software Rules**. The Software Rules page appears. The default tab for this page is Updaters.
3. Click the **Directories** tab. The table of Trusted Directories appears:

Name	Computer Name	Path	Status	Progress
Authorized Downloads	MYCORP\SERVE-2	d:\downloads	Enabled	132/132
WSUS Client updates	MYCORP\WSUS	c:\program files\update services\selfupdate\	Enabled	2246/2339
WSUS Repository	MYCORP\WSUS	f:\wsus\	Enabled	18197/18272

4. Click the **Add Trusted Directory** button. The Add Trusted Directory page appears:

**Add Trusted Directory**

Trusted Directory Settings

Name:

Computer:

Directory:

Description:

Status:  Enabled  Disabled

5. Enter information about the deployment server and the status of the trusted directory. The table below shows the trusted directory fields and their possible values.

**Table 37:** Trusted Directory Parameters

Field	Description
<b>Name</b>	Name used to identify the automatic approval instance in the Trusted Directories table. This can be any text.
<b>Computer</b>	<p>Agent-managed computer that is or will be your software deployment server. This name should match the computer as it appears on the Computers page. For computers in domains, this should include both the domain and the computer name, in one of the following formats:</p> <ul style="list-style-type: none"> <li>• DOMAIN_NAME\computer_name (Windows only)</li> <li>• computer_name.domain.extension (all platforms)</li> </ul> <p><b>Note:</b> If you edit the computer name for an existing Trusted Directory and the Bit9 Server has seen multiple computers by the new name, trusted directories are created for each one.</p>
<b>Directory</b>	<p>Deployment directory for the deployment server. Depending on the deployment technology, you may need to separately specify more than one deployment directory. For example, Microsoft WSUS requires the following directories (substitute actual drive letters):</p> <p>C:\WSUS\WsusContent\  C:\Program Files\Update Services\Selfupdate\  <b>Note:</b> Use of removable drives for trusted directories is not recommended. Removable drives are not re-scanned when removed and reattached, so new software might not be trusted.</p> <p><b>Platform Note:</b> When you enter a path, be sure to use the correct directory delimiters, and to use only characters and formats legal for paths in the chosen platform. The Bit9 Server does not convert paths between platforms (e.g., '\ to '/). Also, keep in mind that Linux files and paths normally are case sensitive.</p>
<b>Description</b>	Optional additional description of this trusted directory.
<b>Status</b>	<p>Select one of the following:</p> <p><b>Enabled</b> – Software present in the trusted directory on the deployment server will be approved for installation on all computers.</p> <p><b>Disabled</b> – Software present in the trusted directory on the deployment server will not be approved for other computers. Software installed from this directory will be treated according to the settings of the policy to which the deployment server belongs.</p>

6. Click the **Save** button. The approval computer and specified configuration information appear in the Trusted Directories table.

**Note**

If you did not enable the trusted directory when you created it, you need to do so before you can use it.

7. Deploy software according to your established procedures. If you want to use the trusted directory to approve Mac or Linux applications, see [“Mac and Linux Trusted Directories”](#) on page 229.

When you enable a trusted directory:

- All files (including files in subfolders) actually present when the trusted directory was enabled are globally approved, as are any files you add after you enable the trusted directory.
- Files identified as installers in Windows trusted directories are globally approved, and files they write are locally approved when and where they are written. Similarly, archive files are globally approved and the files they will write when expanded are globally approved.
- The computer on which the directory resides is configured for permanent prioritization of updates so that any rule changes are applied to it as soon as possible. This status can be changed on the Computer Details page.

#### Note

If you make an existing Windows deployment folder a trusted directory, the Bit9 scanning process that analyzes and approves the directory's contents can take several hours to complete if the folder contains a large amount of software.

## Verifying Trusted Directories

There are several ways you can confirm that a trusted directory is working, and that files in it are being approved.

#### To check the status of a trusted directory:

1. On the console menu, choose **Rules > Software Rules**, and on the Software Rules page, click the **Directories** tab. The table of Trusted Directories appears, and shows the status of each trusted directory and the number of files (of the total) analyzed so far.
2. If you choose, you can click the View Details (file and pencil) button next to a trusted directory to view just the details for that directory. This details page may include additional status information.

You also can check the Events page for trusted directory-related events. There are event subtypes that show directory creation and modification activity as well as the results of any file analysis that occurs in the trusted directory.

To verify that the files on the deployment server are being approved, you can choose **Approved Files** from the Saved Views menu on the File Catalog tab and search for one of the files you expect to see approved. How quickly newly approved files from a trusted directory appear in the Approved Files table depends upon the number of files in the directory and the amount of other activity on the Bit9 Server. To update the Approved Files table, use the Refresh Page button on the File Catalog page.

You also can add a filter to the Approved Files view to see all files approved because of trusted directories. On the Add filter menu, choose **File State Reason**, and then complete the filter by choosing **is** and **Trusted Directory** from the File State Reason menus.

## Verifying Approval of Windows Packages

For Windows installers, you can verify that Bit9 recognized and approved the installer in a trusted directory (and so will locally approve files it installs). On the File Catalog tab, the Saved View called **Trusted Packages** lists installers that are globally approved because they are in a Trusted Directory. This list also includes the Bit9 Agent installers. Files that are not recognized as installers will not appear in this table.

In the Trusted Packages view, click the View Details button (pencil and file) next to a package name to display its File Details page. Click the package name for a table of associated files written by the package.

## Custom Rules for Installer Access

The Bit9 Security Platform supports a Custom Rule that creates a “trusted path.” A trusted path can be useful as a network location in which you place installers so that computers in some or all policies can execute them.

The local state of any files written by a file in a trusted path depends upon the *Execute Action* command used. If the Execute Action is *Allow*, an installer is allowed to write files but those files are not locally approved by the action. If the Execute Action is *Allow and Promote*, the installer can write files and those files will be locally approved (unless already banned). In either case, the global state of any files written is unaffected by the trusted path. See “[Trusted Paths](#)” on page 367 for more details.

## Removing or Disabling Directory Trust

If you decide to remove trust from a trusted directory, you can do one of two things:

- You can *disable* the trusted directory so that files added *after* you disable it are no longer trusted. You do this by clicking the View Details (pencil and file) button next to its name, clicking the **Disabled** status radio button, and then clicking **Save**. Consider this if you want to temporarily suspend installations from your deployment server. Disabling (rather than deleting) gives you the option of re-enabling the directory at a later time without having to reenter all of its properties.
- You can *delete* the directory from the Trusted Directories list by clicking the **X** button next to its name. This deletes its *trusted status* in Bit9, not the actual folder. Delete the folder itself if you do not want its contents on your deployment server.

### Notes

- Disabling or deleting trusted directory status does not remove approval from files that were already in the directory.
- A Trusted Directory folder that is either deleted from the computer or inaccessible to Bit9 Agents due to network issues is listed as *Enabled, Inaccessible* in the Trusted Directories table.

## Approving by Trusted User or Group

The Bit9 Security Platform supports installation privileges for users who need to install software on their own or others' computers when the computers are under High Enforcement protection. You can trust individual users or specify trusted groups whose members become trusted users.

Trusted users and users in trusted groups have full permission to install software (unless banned) on any accessible computer that allows them to log in with their credentials. Applications installed by a trusted user are locally approved where they are installed.

### How Groups are Specified

For Mac and Linux, you specify a group by entering its name.

For Windows, you have the following choices for specifying a group:

- If AD is implemented, you can specify an AD group. You enter it by typing in the group and domain name, or an SID.
- You can pick a built-in Windows group from a menu.

If you choose AD users or groups:

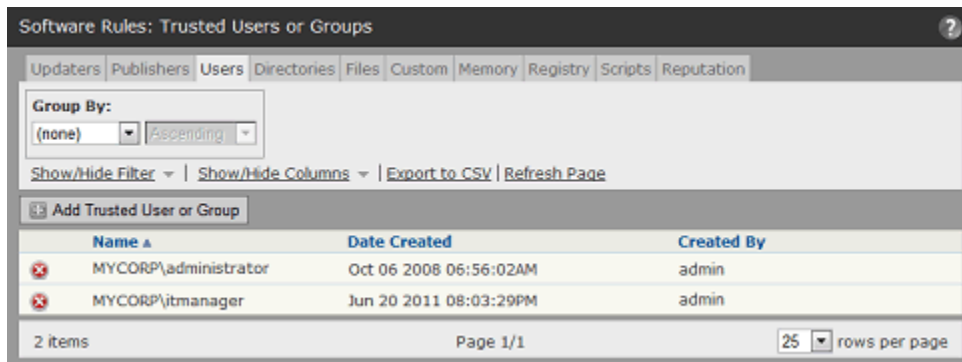
- You can specify trusted AD users or groups as long as the Bit9 Server has access to AD information about that user or group.
- AD-based privileges are determined when a user logs in. If you change an AD group in a way that affects Bit9 privileges, any logged-in users in that group are not affected until the *next* time they log in.

If you choose a built-in Windows group, certain operating system versions may not provide the access you expect. When running on Windows Vista and later, membership in pre-defined security groups like Administrators requires that the application run as an administrator. If a group definition is necessary for a rule, consider using security groups *you* have defined rather than the pre-defined groups.

### Creating a Trusted User or Group

**To designate users who can install software on High Enforcement Level computers:**

1. On the console menu, choose **Rules > Software Rules** and click the **Users** tab on the Software Rules page. The Trusted Users or Groups view appears.



2. Click the **Add Trusted User or Group** button. The Add Trusted User or Group page appears:

The screenshot shows the 'Add Trusted User or Group' dialog box. The title bar reads 'Add Trusted User or Group'. Below the title bar is a text input field labeled 'Enter name of trusted user or group'. The 'Platform' dropdown menu is set to 'Windows'. Under 'Create Trust Type', the radio button for 'User or group' is selected, and 'Pre-defined group' is unselected. There is an empty text input field for 'User Or Group Name'. At the bottom, there are 'Save' and 'Cancel' buttons.

3. Choose the Platform from which you will choose a use or group. Some of the fields change if you choose Mac or Linux instead of Windows.

The screenshot shows the 'Add Trusted User or Group' dialog box. The title bar reads 'Add Trusted User or Group'. Below the title bar is a text input field labeled 'Enter name of trusted user or group'. The 'Platform' dropdown menu is set to 'Mac'. Under 'Create Trust Type', the radio button for 'User' is selected, and 'Group' is unselected. There is an empty text input field for 'User Or Group Name'. At the bottom, there are 'Save' and 'Cancel' buttons.

4. If you chose Windows as the platform, enter the name of the user or group to be given trusted privileges in **one** of the following ways:
  - Leave **User or group** checked and enter a valid domain and user name in either of these formats: *DOMAIN\_NAME\user\_name* or *user\_name@DOMAIN\_NAME*
  - Leave **User or group** checked and enter a valid AD group name in either of these formats:  
*DOMAIN\_NAME\group\_name* or *group\_name@DOMAIN\_NAME*
  - Leave **User or group** checked and enter a valid User or Group SID.
  - Click the **Pre-defined group** button and choose a Windows group from the menu.

The screenshot shows the 'Add Trusted User or Group' dialog box. The title bar reads 'Add Trusted User or Group'. Below the title bar is a text input field labeled 'Enter name of trusted user or group'. The 'Platform' dropdown menu is set to 'Windows'. Under 'Create Trust Type', the radio button for 'Pre-defined group' is selected, and 'User or group' is unselected. The 'Group' dropdown menu is open, showing a list of Windows groups: 'Authenticated Users', 'Backup Operators', 'Local Administrators', 'Local Service', 'Local System', 'Network Configuration Operators', 'Network Service', 'Power Users', and 'Service Accounts'. At the bottom, there are 'Save' and 'Cancel' buttons.

5. If you chose Mac or Linux as the platform, enter the name of the user or group to be given trusted privileges in **one** of the following ways:
  - Leave **User** selected and enter a valid user name for the platform you chose.
  - Click **Group** and enter a valid group name for the platform you chose.
6. Click the **Save** button. The user or group appears in the Trusted Users table.

## Removing Trust from a User or Group

If you no longer want a user or group to have installation privileges on locked-down computers, you can remove that user or group from the Trusted Users or Groups table. You do this by clicking the Delete (X) button next to the entry for that user or group.

### Important

- If you eliminate Bit9 trust from a user or group, that user or group loses its trusted status almost immediately, as soon as Bit9 Agents receive the change. This means the user is not trusted to perform new installations. However, a process that was created when the user was trusted remains trusted until the process exits.
- If you remove a user from an AD group that is trusted by Bit9, the user continues to be trusted until he or she logs out.

## Approving or Banning by Publisher

### Platform Note

Publisher approvals and bans currently work only on Windows computers. They have no effect on files on other platforms.

Many files are signed with a digital certificate that verifies the integrity and identity of the file, including the name of its publisher. The Publishers tab of the Software Rules page lists each unique publisher identified in a valid certificate for a file discovered by a Bit9 Agent. If Windows can find the digital signature on a file, the publisher should be discovered and listed in the Bit9 Console.

Once a publisher is listed in the Bit9 Console, it may be approved, banned, or left unapproved. Publisher approvals and bans can be applied to all computers or to computers in specific policies. You may Acknowledge a publisher to indicate that you have seen it and do not need to track it as closely. Acknowledging a publisher does not change its state.

Publisher state affects files differently depending upon whether you have banned or approved the publisher:

- **Bans** – When you ban a publisher, any file signed by a certificate identifying that publisher is banned.
- **Approvals** – When you approve a publisher, a file signed by a certificate identifying that publisher is approved *if its certificate meets additional Bit9 validation requirements*. These requirements are described in more detail in the section [“Determining Which Certificates Can Approve Files”](#) on page 242.



**Note**

The Bit9 Platform also allows approval or banning of certificates themselves. This is a more secure but more complex way to identify and control files by identifying their source. See [Chapter 10, “Managing File-Signing Certificates,”](#) for more details.

## Publisher Approvals

You might approve files by publisher when it is not practical to approve applications using a trusted directory and you want to permit all users to install all software from a particular source. Applications from approved publishers are permitted to be installed and run on computers in the policies to which the approval applies. The Global State of publisher-approved files is changed (if necessary), but the File State is not changed (see [“Global File State”](#) on page 217). Each instance of such files is locally approved, and therefore allowed to run on the computer on which it is present.

Approving by publisher allows you to assure that new files from a trusted source are pre-approved when they arrive on an agent-managed computer. It also can reduce the amount of rule traffic sent to agents since it is not necessary to send an individual rule for each file.

There are two ways to approve a publisher:

- **Manual Approval** – You can choose to approve publishers that you select from the list on the Publishers tab. Manual approval is described in this section.
- **Reputation Approval** – You can enable automatic approval of all publishers that meet a particular trust threshold as reported by Bit9 SRS. Approving a publisher by reputation has the same effect on *existing* files as approving it manually. In addition, as soon as a file with a new publisher is discovered on one of your computers, the publisher is approved if it is known to Bit9 SRS and meets the trust level you chose. Specific instructions and considerations for reputation approval of publishers are described in [Chapter 9, “Reputation Approval Rules.”](#)

**Important**

Before approving a publisher, consider all possible files that could come from that publisher. Once the approval is added, *all* executables and script files from the publisher will be locally approved. You can remove the publisher from the Approved list, but this only affects files not yet encountered on your network at the time of the change – there is no single operation to remove *file* approval from all files already locally approved because of a publisher approval.

## Publisher Bans

When you ban a publisher, agent computers in policies affected by that ban cannot run software from that publisher. You might ban files by publisher when you know that the publisher is a source of malicious files or applications that you simply don’t want running in your environment. When you create a publisher ban, the local state of files from that publisher is changed to Banned.

You can ban files by publisher even if they are invalidly signed or do not meet other requirements for approval by publisher.

Publisher bans are created manually through the Bit9 Console.

**Important**

As with approvals, consider all of the files that might be affected by a publisher ban and be sure that a publisher ban does not inadvertently ban a file required in your environment.

## Managing Bans and Approvals from the Publishers Tab

On the Publishers tab, you can approve, ban, or remove bans and approvals from multiple publishers at one time. Publisher state changes performed from this table apply to all policies.

When you check more than one publisher in the table, you must perform the same state change on them; that is, you must ban them all, approve them all, or remove the ban or approval on all. You cannot ban some publishers and approve others in a single operation.

**To approve or ban software from one or more publishers for all policies:**

1. On the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click the **Publishers** tab. All publishers of validly signed software discovered on agent-managed computers reporting to your server, plus any publishers whose certificates you added manually, appear in the Publishers table:

Name	Date Approved	Approved By	Trust	State Reason
State: Approved 22 items				
Adobe Systems Incorporated	Nov 29 2011 09:53:09AM	rjones@mycorp.local	High	Manual
Adobe Systems, Incorporated	Nov 29 2011 09:53:13AM	rjones@mycorp.local	High	Manual
Bit9, Inc	Jun 01 2010 11:45:59AM	System	High	Manual
Bit9, Inc	Jun 01 2010 11:45:59AM	System	High	Manual
Dell Inc	May 09 2007 07:22:06AM	dgomez@mycorp.local	High	Manual
Dell Inc.	May 09 2007 07:22:18AM	dgomez@mycorp.local	High	Manual

3. In the table of publishers, locate the publishers you want to approve, or the publishers you want to ban. Keep in mind that the table may be several pages long.

**Note**

Files from the same company can be identified as being from different publishers, often based on minor changes in punctuation. These appear as separate lines in the Publishers table. For example, you might see both “Adobe Inc.” and “Adobe, Inc.” in the table. You can approve (or leave unapproved) each instance separately. If files signed by a publisher appear as unapproved on the Files page and you want these files approved, be sure to approve the correct version of the publisher certificate.

4. Review the publisher(s) you are interested in approving or banning. If necessary, open the Publisher Details page for specific publishers for more information.
5. Check the checkbox next to the name of each publisher whose state you want to change. You can check as many names as you want on one page. Note that approval and ban actions are applied to the currently visible page only.
6. When you have checked all the publishers (on the current page) whose state you want to change, on the Action menu:
  - a. Choose **Approve Publishers** to approve all of the selected items.
  - b. Choose **Ban Publishers** to ban all of the selected items.
  - c. Choose **Remove Approval or Ban** to return all selected publishers to the Unapproved state.

## Managing Bans and Approvals from the Publishers Details Page

For a single publisher, you can use the Publisher Details page to approve or ban the publisher, or to remove an approval or ban. You also can change the policies to which an approval or ban applies.

### To approve or ban one publisher in some or all policies (Publisher Details page):

1. On the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click the **Publishers** tab. All publishers of validly signed software discovered on agent-managed computers reporting to your server, plus any publishers whose certificates you manually added, appear in the Publishers table.
3. From the table of publishers, locate the publisher whose state you want to modify and click on the View Details button (pencil and file). The Publisher Details page opens.
4. In the State field, choose **Approved** or **Banned**.
5. If you choose, change the Acknowledged state to **Yes**. This indicates that you have reviewed the publisher so that you can concentrate on publishers you haven't yet reviewed. To do this, you can filter the Publishers table using the Acknowledged field. Acknowledging a publisher has no impact on its approval state.
6. In the Rule Applies To field, click the radio button for **All policies** or **Selected policies**.
7. If you chose *Selected policies*, check the box next to each policy for which you want the publisher approval or ban to be enabled.
8. In the Platforms field, click the radio button for **All platforms** or **Selected platforms**. **Platform Note:** Publisher approvals and bans currently affect only Windows agents.
9. When you are finished configuring the approval or ban, click the **Save** button.

## Adding Publishers

Any publisher already identified through a file on a computer running the Bit9 Agent should appear in the Publishers table, but you might want to approve a publisher before its files arrive on your computers. This could be the case, for example, if you distribute software using a computer that does not run the Bit9 Agent. To address this, you can *manually* add publishers to the table.

### To add a publisher:

1. Open a browser and log in to the Bit9 Console on a computer with access to the file whose publisher you want to add. It might be most convenient to do this on the computer that has the file.
2. On the Publishers tab, click the **Add Publisher** button to view the Add Publisher dialog:



3. Click the **Browse** button and locate an application file validly signed by the publisher. You can browse to any validly signed, executable file and add its publisher:
4. In Windows, confirm that the file is signed by right-clicking on the file and choosing Properties from the menu. If there is a Digital Signatures tab on the Properties window, the file is signed and you can examine its credentials.
5. Double-click the filename to enter it into the File Name field.
6. Click the **Save** button. Publisher information is extracted and the publisher is added to the table, initially in the Unapproved state.
7. If you want to approve or ban this new publisher for all policies, check the box next to its new entry in the Publisher table and choose **Approve Publishers or Ban Publishers** from the Action menu. The publisher is approved, and if you have the table grouped by State, the publisher moves into the appropriate *State* section. Now, as soon as a file from this publisher appears on one of your agent-managed computers, it will be handled as you instructed.

You also can approve or ban the publisher by policy from the Publisher Details page.

### Note

When you add a publisher manually, the Bit9 Server creates a temporary copy of the file you identified and then deletes it after the publisher has been added. If an agent is running on the server computer, the file will appear in the File Catalog, but will have a prevalence of zero.

## Removing Publisher Approvals

To change an *approved* publisher to *unapproved*, go to the Publisher tab on the Software Rules page, check the box next to its name and choose **Remove Publisher Approval** on the Action menu. This simply removes approval; it does not ban the publisher. You also can remove approval using the Publisher Details page.

Any computers that have installed or run software from this publisher while it was approved continue to be able to run the software. All existing instances of software from an approved publisher are locally approved, and the local approval is not removed by the change in publisher status on the Bit9 Server.

## Removing Publisher Bans

To change a *banned* publisher to *unapproved*, go to the Publisher tab on the Software Rules page, check the box next to its name and choose **Remove Publisher Approval or Ban** on the Action menu. This simply removes the ban; it does not approve the publisher. You also can remove the ban by choosing **Unapproved** in the State menu on the Publisher Details page.

When a publisher ban is removed, the files from that publisher revert to whatever their state would have been without the publisher ban.

## Finding All Files from a Publisher

On the Publishers tab of Software Rules, you can find all instances of files on your computers that are identified as being from a specified publisher. You do this by clicking the Find Files button next to the publisher name. You also can get this list using the Related Views menu on the Publisher Details page.

## Determining Which Certificates Can Approve Files

Publisher identification and approval of files by publisher approval are both based on digital certificates. If you are unfamiliar with certificates, the following web sites may provide useful background:

[http://msdn.microsoft.com/en-us/library/ms537361\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms537361(v=vs.85).aspx)

<https://sites.google.com/site/ddmwsst/digital-certificates>

It is important to distinguish between approval of a publisher and approval of a file identified as being from that publisher. You can approve any publisher that appears on the Publishers tab of the Software Rules page. A publisher appears in this list if a file had a certificate identifying the publisher and the signature was considered valid by Windows.

However, a *file* identified as being from this publisher can be approved by publisher only if all certificates in the certificate chain for that file are considered valid by Windows. For example, current root certificates must be installed for a certificate to be accepted.

**Note**

Microsoft security bulletin MS13-098 describes a flaw in the Authenticode signature verification that could allow remote code execution. In response, Microsoft announced availability of an update for all supported releases of Windows to change how signatures are verified for binaries signed with the Windows Authenticode signature format. If this change is enabled, Windows Authenticode signature verification will no longer allow extraneous information in the WIN\_CERTIFICATE structure, and Windows will no longer recognize non-compliant binaries as signed. Activation of this new behavior could cause files previously approved by publisher to block on Bit9-managed systems.

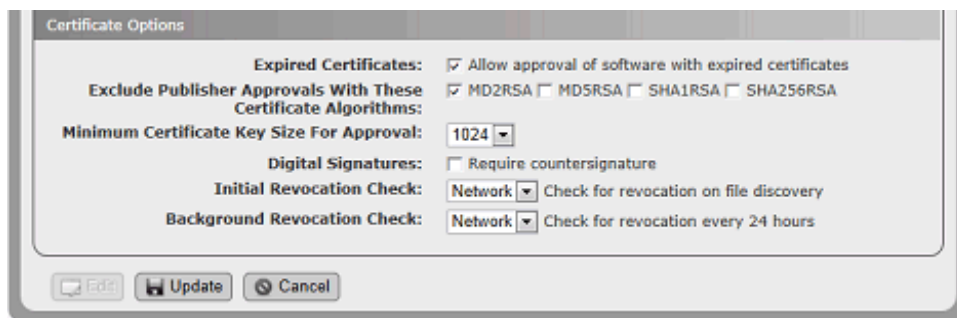
The change is included with Security Bulletin MS13-098, but (as of July 2014) will only be enabled on an opt-in basis. However, Microsoft states that it may make this a default behavior in a future release of Microsoft Windows. See <https://technet.microsoft.com/library/security/2915720> for more information on this change.

All certificates in the chain for a file must also meet additional Bit9 requirements. These settings are configurable on the Advanced Options tab of the System Configuration page. Keep the following in mind about these certificate settings:

- It is best to set certificate configuration options *before* generating the agent installation packages (i.e., as soon as possible after installing Bit9 Server). This assures that all agents, including those disconnected from the server, will handle certificates as you want them to. In addition, changing certificate settings after the agent is installed requires re-evaluation of certificates to occur on each agent. Having these settings correct before deploying the agent avoids a significant amount of processing.
- Changing any of the configurable certificate settings does not remove local approval of files whose certificates met the previous settings and were approved by publisher.
- Changing certificate settings may affect the tracking and inventory of Microsoft Support Files. See “[Changes that Affect OS Inventory Tracking](#)” on page 200.

**To view and change configurable certificate approval options:**

1. On the console menu, choose **Administration > System Configuration**.
2. On the System Configuration page, click **Advanced Options** on the menu. The Advanced Options Configuration page appears, with the Certificate Options panel at the bottom.





3. At the bottom of the page, click the **Edit** button.
4. **Expired Certificates:** In the Certificate Options panel, use of expired certificates is enabled by default. See “[Approval with Expired Certificates](#)” on page 244 for information that may assist you in configuring this option:
  - a. To *disable* the use of expired certificates, *un-check* the *Expired Certificates* checkbox.
  - b. To *re-enable* use of expired certificates after it has been disabled, check the box.
5. **Exclude Publisher Approvals With These Certificate Algorithms:** Review the currently checked boxes in this field. See “[Excluding Certificate Algorithms](#)” on page 245 for information that may assist you in configuring this option.
  - a. To *prevent* publisher approvals of files signed by certificates with a certain algorithm, check the box next to the algorithm name.
  - b. To *allow* publisher approvals of files signed by a certificates with a certain algorithm, *un-check* the box next to the algorithm name.
6. **Minimum Certificate Key Size for Approval:** To change the minimum certificate key length required for a file to be approved by publisher, choose a new value from the menu. See “[Minimum Key Size](#)” on page 245 for information that may assist you in configuring this option.
7. **Digital Countersignatures:** To require a countersignature for the digital signature of each certificate, check the *Require countersignature* box. If you do not want to require a countersignature, *un-check* the box. See “[Countersignature Options](#)” on page 245 for information that may assist you in configuring this option.
8. **Initial/Background Revocation Check:** Two separate settings control checks for certificate revocation: *initial*, which controls the revocation check when a file is first discovered, and *background*, which controls ongoing checks that occur (if enabled) every 24 hours. See “[Revocation Checks](#)” on page 245 for information about these settings.
9. If you changed any settings, click the **Update** button at the bottom of the page and in the Confirm Server Setting Change dialog, click **Yes** to save your changes.

## Approval with Expired Certificates

By default, the Bit9 Security Platform allows the use of expired certificates whose (verifiable) timestamp is within the certificate validity period to approve files by publisher. If the timestamp is missing, invalid, or is before or after the certificate validity period, then the software cannot be approved by publisher.

You can disable approval by expired certificates that would otherwise be trusted by the Bit9 Security Platform. This provides extra security, but can prevent approval of legitimate files whose valid certificate is now out of date.

When you disable *Allow approval of software with expired certificates*, all publishers are re-evaluated. However, if a file was locally approved by a publisher with an expired certificate when this was allowed, it remains locally approved when the setting is disabled.

The Expired Certificates setting has no effect on *bans* of publishers, so you can ban files by publisher even if they have an invalid signature or an expired certificate.



**Important**

It is especially important to set the expired certificate option before generating installation packages for agents that will be primarily or permanently disconnected from the server. This assures that disconnected agents will handle expired certificates as you want them to.

**Excluding Certificate Algorithms**

With the *Exclude Publisher Approvals With These Certificate Algorithms* option, you can disallow publisher-based approval of files whose certificates use certain algorithms. If an algorithm box is checked, files whose certificates use that algorithm *cannot* be approved by publisher. If not checked, a certificate using that algorithm may be used to approve files by publisher. The choices are: MD2RSA, MD5RSA, SHA1RSA, and SHA256RSA. The default for new Parity installations beginning with 7.0.1 Patch 11 is to allow certificates with any of the listed algorithms to be used for approvals. Upgrades and patches from previous releases also allow certificates with any of the listed algorithms to be used for approvals unless the setting was modified through the console before the upgrade.

**Minimum Key Size**

The *Minimum Certificate Key Size for Approval* option allows you to specify a minimum key length for a certificate to be used for file approval. Choices range from 512 to 4096. Certificates whose key size is greater than or equal to the chosen value may be used to approve files. Certificates whose key size is smaller than the chosen value may not be used for file approval. The default value for new Parity installations beginning with 7.0.1 Patch 11 is 512. Upgrades and patches from previous releases also use this value unless the setting was modified through the console before the upgrade.

**Countersignature Options**

You can choose to require that the digital signature for a certificate is countersigned in order for Bit9 to approve a signed file by publisher. This can provide greater security against manipulation of time stamps on a signature. By default, the box is not checked (i.e., no countersignature is required). If the box is checked, certificates that are not countersigned are not considered valid for use in approval by publisher.

Note the following additional details of countersignature handling:

- If the box is unchecked, signatures lacking a countersigner are only valid for the life of the signing certificate.
- Regardless of this setting, if a countersignature is present, it must be valid for the digital signature to be considered valid.

**Revocation Checks**

There are two settings that control if and how the agent checks to see whether a file's certificate has been revoked:

- **Initial Revocation Check** – This determines whether, and if so, how a certificate revocation check is done when a file is initially discovered on an agent.
- **Background Revocation Check** – This determines whether, and if so, how a certificate revocation check is done in the background every 24 hours.

For each of the revocation settings, there are three possible values:

- **Network** – If revocation information is not locally available then use the network to retrieve the revocation status of a certificate.
- **Cache** – Use locally available revocation status information when performing certificate revocation (the network will not be used).
- **None** – Do not perform certificate revocation checking.

Consider your agent deployment scenario when setting these values since they can impact agent performance. For example, if you have offline agents, you might want to avoid using the Network option, especially for the Initial Revocation Check. Also keep in mind that the daily revocation check is performed in the background, and is less likely to have a negative impact on agent performance, whereas the initial revocation check setting may have a noticeable effect on agent performance.

#### Note

Regardless of whether agent-based certificate revocation checks are enabled, the Bit9 Server validates certificates in its inventory on a recurring basis to make sure that they have not been revoked. This validation generally occurs on a weekly basis and involves downloading certificate revocation lists (CRLs) from registration authorities or making Online Certificate Status Protocol (OCSP) calls to OCSP responders. If you are monitoring network traffic, keep in mind that these downloads might involve a variety of sites in a variety of countries.

Server-based validation checks are provided to inform administrators when the status a certificate changes, but they do not affect enforcement of rules. Enable agent-based revocation checks if you want revocations to affect rule behavior.

## Approving by Updater

Updater Approval Rules permit users of computers under High Enforcement protection to install application updates from approved sources as they become available for download. You can approve updater programs for commonly used enterprise applications, including anti-virus, anti-spyware, personal firewall, and desktop productivity programs. All computers can run approved updaters, but applications installed by these updaters via the Web are locally approved by the Bit9 Agent for use on the installation computer only.

**Platform Note:** Updaters are platform-specific. Most of the updaters are disabled by default but can be enabled. Prior to version 7.2.1, the built-in updaters for Mac and Linux were not listed but were enabled automatically. They are now listed as separate updaters and disabled by default to allow greater control of your environment. The Mac App Store Downloads is one of the few updaters enabled by default, but you may disable it.

The standard Updaters tab lists three types of “updaters”:

- Updaters for a specific product or product family (such as "Google Chrome").
- Special purpose items, such as an “updater” that allows writing of files from software distribution systems (e.g., "Microsoft SCCM").

- Some “updaters” are actually delivery mechanisms for special Bit9 functionality. For example, there are “updaters” that are sets of tamper protection rules for the Bit9 Server and the Carbon Black sensor, respectively. You can enable them for extra protection or disable them if they interfere with activities you need to perform on the server or an endpoint.

Keep in mind that enabling a product-specific updater approves only the *upgrade procedure* for that product, not the application's full installation package.

As new applications or new application versions are introduced, and old products or versions become obsolete, the list of updaters you need may change. The list of available updaters is refreshed in the following ways:

- When you install a new version of the Bit9 Security Platform, the updaters list is refreshed to add any new updaters, delete any obsolete updaters, and make any necessary modifications to existing updaters.
- To keep your updaters current, you can allow automatic updating of your updaters by Bit9 SRS (enabled by default when Bit9 SRS is enabled).
- For update programs currently not supported, you can contact Bit9 to request an addition to the list. If approved and made available, the new updater can be manually added to your Bit9 Server or downloaded automatically through the Bit9 SRS.

### Notes

To avoid unwanted file blocking, before you install any Bit9 Agents, it is best to enable any supported updaters for any applications your organization runs. If an updater that is not enabled attempts to modify files, and this results in the application being blocked, you can use global or local approval methods to manually approve the blocked files.

You can view the complete list of updaters available on your server by opening the Software Rules Updaters page on the console. In addition to supported v7.2.1 updaters, this page might show a manually added updater or, if you have upgraded from a previous version of Bit9 (Parity), older updaters you have enabled in the past.

[Table 38](#) provides information about updaters whose names might not make their purpose obvious or that require special implementation notes. If you do not have access to the Bit9 Console and need a complete list of supported updaters, contact Bit9 Technical Support.

**Table 38:** Updater Notes

Updater	Platform	Description
<b>Note:</b> This table describes only updaters requiring addition explanation. For a complete list of updaters, see the Software Rules/Updaters page in your console.		
<b>Adobe Application Manager</b>	Windows	Allows updates of products <i>managed by</i> the Adobe Application Manager.
<b>Adobe Products Not Listed</b>	Windows	Allows automatic approval of updates to certain Adobe products for which a specific Bit9 updater is not shown.

Updater	Platform	Description
<b>Allow Printer Installations</b>	Windows	Allows a print server to automatically install a printer driver not currently on an agent computer (Windows 2003 and later). This updater should not be enabled as a means to allow installation of drivers for locally attached printers.
<b>Bit9 Server Tamper Protection</b>	Windows	This “updater” is actually a set of rules to protect the Bit9 Server from tampering. It is disabled by default, but enabling it is recommended for extra protection. It may be disabled later if necessary for troubleshooting purposes.
<b>Carbon Black</b>	Mac	Allows updates to the Carbon Black sensor on endpoints running OS X.
<b>Carbon Black Tamper Protection</b>	Windows	This “updater” is actually a set of rules to protect the Carbon Black sensor from tampering. If you have both the Bit9 Agent and the Carbon Black sensor installed on endpoints, enabling this updater provides extra protection.
<b>CSC.exe Temporary Files - Do Not Report</b>	Windows	This updater significantly reduces the number of new file reports on the server when the Microsoft Visual C# Compiler (CSC.exe) creates or modifies DLLs in locations dedicated to temporary files. You may still approve or ban files at these locations when this “updater” is enabled, and you can disable it if you prefer to see all temporary file traffic from this process.
<b>Java</b>	Windows	Allows updates to the Java Virtual Machine and updates that install or update add-ons (search bars or third-party applications, etc.) included in some versions of Java. This is equivalent to the Java and Bundled Software updater from previous releases.
<b>Mac System Updates</b>	Mac	Allows updates to the OS X operating system. <b>Note:</b> In pre-7.2.1 releases, Mac System Updates were automatically allowed and there was no updater listed. You can now control whether these updates are allowed.
<b>Microsoft .NET Framework</b>	Windows	Allows the .NET just-in-time compiler to run. It must be enabled if you run any applications that require .NET.  Although <b>Windows Update</b> provides updates for both <b>Windows Defender</b> and <b>Microsoft .NET</b> , successful installation of updates for either of these products requires that you trust their specific updater in addition to Windows Update.
<b>Microsoft Office 2013</b>	Windows	Allows updates based on Microsoft's Click-to-Run streaming technology. If you used the MSI installer for Office and did not enable Click-to-Run, Office updates will be provided by Windows Update and this updater does not need to be enabled.

Updater	Platform	Description
<b>Red Hat Prelinking</b>	Linux	Bit9 recommends disabling Prelinking on RedHat and CentOS computers before installing agents. Prelinking has negative impacts on performance and Bit9 features (see the Release Notes). However, if you must enable Prelinking on your RedHat and CentOS systems, enable the RedHat Prelinking updater before installing agents.
<b>Red Hat Software Update</b>	Linux	Allows automatic updates to supported RedHat and CentOS operating systems.
<b>Symantec Endpoint Protection for Mac</b>	Mac	Enable the <b>Symantec Endpoint Protection for Mac</b> updater if SEP is run in your environment. It allows SEP updates and improves performance on file operations. Use the SEP Auto Protect Preferences Pane to configure SEP to include the following endpoint SafeZone: <b>/Library/Application Support/com.bit9.Agent</b>
<b>Ubuntu Software Update</b>	Linux	Allows automatic updates to supported Ubuntu operating systems.
<b>Windows 8 and Server 2012 Updates</b>	Windows	Allows updates for these platforms on pre-7.0.1-Patch 11 agents. These updates are enabled automatically on all 7.2.0 and 7.2.1 agents and in 7.0.1 Patch 11 agents and later.
<b>Windows Defender</b>	Windows	Although <b>Windows Update</b> provides updates for both <b>Windows Defender</b> and <b>Microsoft .NET</b> , successful installation of updates for either of these products requires that you trust their specific updater in addition to Windows Update.
<b>Windows Update (for pre-6.0.2 agents)</b>	Windows	This updater allows Windows Updates to run on pre-6.0.2 agents. Windows Updates are enabled by default for v6.0.2 and later agents.
<b>Windows Update Temporary Files - Do Not Report</b>	Windows	This updater significantly reduces the number of new file reports on the server when Windows updates are applied. Since the files not reported are in temporary locations and supplied by Microsoft, they should not be of interest for tracking or investigation. You may still approve or ban files at these locations when this “updater” is enabled, and you can disable it if you prefer to see all updater file traffic.

**To specify automatic approval of software installed by application updaters:**

1. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click the **Updaters** tab. A table of updater programs for various applications appears, grouped by default according to whether they are enabled:

Name	Enabled	Date Created	Created By	Date Modified
<b>Enabled: Yes</b> 23 items				
<b>Enabled: No</b> 12 items				
Adobe Acrobat Reader 10.0	No	Jan 26 2012 09:32:21AM	System	Jan 30 2012 06:28:43PM
Adobe FrameMaker	No	Jan 26 2012 09:32:18AM	System	Jan 30 2012 06:20:39PM
Allow Printer Installations	No	Jan 26 2012 09:32:21AM	System	Jan 30 2012 06:28:43PM
BigFix Enterprise Client	No	Jan 26 2012 09:32:21AM	System	Jan 26 2012 09:32:21AM
CA ITM	No	Jan 26 2012 09:32:21AM	System	Jan 26 2012 09:32:21AM
Google Chrome	No	Jan 26 2012 09:32:21AM	System	Jan 30 2012 06:28:44PM

3. Check the box on the far left of the row for any currently disabled updaters you want to enable, and then choose **Enable Updaters** on the Action menu. The updaters are enabled and, if you have the default grouping, moved into the *Enabled: Yes* section. Computers running the Bit9 Agent can now install software using the automatic updaters for these applications.

**Note**

Some software manufacturers include multiple products in the same product family. Verify that the updater you select corresponds to the correct product and version for your application.

4. If you would like Bit9 SRS to keep your updater list current with updater changes, additions, and deletions, leave the “updater updates” option enabled. See [“Allowing or Disabling Automatic Updater Updates”](#) on page 251.
5. If an updater you want to include does not appear in the table, you can contact Bit9 Technical Support to submit a request for a new updater. See [“Adding an Updater”](#) on page 251 for more information on adding an updater.
6. To disable updaters, check the box next to the Name of each updater you want to disable and then choose **Disable Updaters** on the Action menu.

## Allowing or Disabling Automatic Updater Updates

Changes in the products or product versions from software providers might change the list of updaters you need. Bit9 tracks changes to the updaters for supported products as well as the arrival of new products with their own updaters. When you install a new version of the Bit9 Security Platform, the updater list is modified to reflect these changes. However, you might need to have the updater list refreshed between releases.

By allowing Bit9 SRS to maintain the updater list, you can get new and modified updaters as soon as they become available from Bit9. Enabling Bit9 SRS updates also means that obsolete updaters are deleted from the updater list. In addition to keeping your updater list current, automatic updates eliminate much of the need for manually updating the updaters on the list. Note that this feature is enabled by default if you have Bit9 SRS enabled.

### To enable or disable automatic updating of updaters by Bit9 SRS:

1. On the console menu, choose **Administration > System Configuration**.
2. On the System Configuration page, click **Advanced Options** on the menu. The Advanced Options Configuration page appears, with the Software Rules Options panel at the bottom.
3. At the bottom of the page, click the **Edit** button.
4. In the Software Rule Options panel, the Bit9 SRS updater option is enabled by default:
  - a. If you *do not want* Bit9 SRS to keep your updaters current, *un-check* the *Automatically update application updaters from Bit9 SRS* box and then click the **Update** button at the bottom of the page.
  - b. If you want to *re-enable* automatic updates from Bit9 SRS after they have been disabled, check the box and click the **Update** button.



5. In the Confirm Server Setting Change dialog, click **Yes** to save your changes.

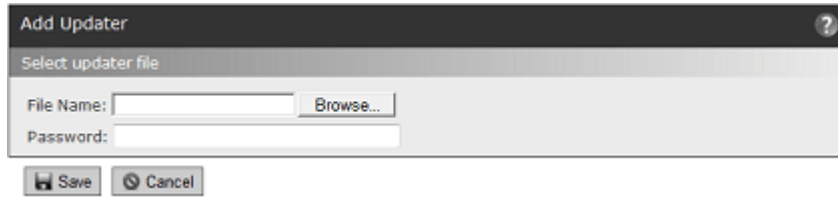
## Adding an Updater

If you need an application or software distribution updater not in the current Updaters table, you can submit a new updater request to Bit9 Technical Support. If the request is accepted, the new updater can be delivered in one of two ways:

- If you have enabled Bit9 SRS updates for your updaters, the new updater can be automatically installed on your Bit9 Server when it is ready.
- The new updater may be supplied to you by Bit9 as an update file.

### To install a new updater from a Bit9-supplied file:

1. Download the updater file according to your support engineer's instructions and put it in a location accessible to your Bit9 Server.
2. On the console menu, choose **Rules > Software Rules** and then click the **Updater** tab
3. Click the **Add Updater** button. The Add Updater page appears:



4. Click the **Browse** button, locate the new updater, and click **Open** on the file chooser. The file pathname appears in the File name box.
5. Click the **Save** button. The new updater is installed but not enabled.
6. To enable the new updater, check the box to the left of its name and then choose **Enable Updaters** on the Action menu. The updater moves into the *Enabled: Yes* section and users can now install software using the updater for this application.

## Updater History

Viewing the history of an updater can show whether it is current and when any modifications were made to it. For example, the *Date Created* field in the history might suggest that Bit9 SRS added a new updater.

### To view an updater's history:

- On the Updaters tab, click the View History button next to the name of the updater. Click the **Return** button to go back to the full list of updaters.

The history page includes the following information about the updater:

- Updater Name
- Platform
- Enabled (Yes/No)
- Updater Version number
- Date Created (on this Bit9 Server)
- Created by (on this Bit9 Server)
- A history of any modifications to the updater

Using the Related Views menu of the Updater History, you can see which agent-managed computers have the latest rule for this updater.

## Locally Approving Files

When the Bit9 Agent is installed on a computer for the first time, the computer goes through an *initialization* process during which all files present on that computer are *locally approved* unless they are already globally approved or banned. This means that they are allowed to run on that computer, regardless of its Enforcement Level. Local approval has no effect on the *global state* of the files, however. By locally approving files present during agent initialization, you can set up a computer with the files it needs to run, saving global decisions about these files for a later time when you have used the Bit9 Security Platform to collect more information about the files and computers on your network.



Files that appear on a computer *after* Bit9 Agent initialization, if not explicitly banned or approved, are assigned *Unapproved* state. Unapproved files are allowed to run on computers running in Low Enforcement and (with user intervention) Medium Enforcement, but they are not allowed to run on computers in High Enforcement.

You might want a particular computer to be able to run a new application without approving it for any other computers on your network. You also might want to change the state of a file from Unapproved to Locally Approved on one or more computers before putting those computers into High Enforcement. To accomplish tasks like these, the Bit9 Security Platform offers the following options:

- A per-policy ability to make certain unapproved files Locally Approved when a computer makes a transition to a more secure Enforcement Level
- Local approval of individual files on a specific computer
- Local approval of all unapproved files on a specific computer
- Temporary reassignment of a computer in High or Medium enforcement to the Local Approval policy, during which any files that are installed are locally approved
- Designation of files as installers even when Bit9 analysis did not identify them as such, and vice versa; local approval of an installer also locally approves all of the files it installs

#### Note

- You cannot use any of these methods to locally approve a file that has been globally banned or that is banned by policy on the computer with the file. You also cannot remove local approval for a file that has been globally approved or that is approved by policy on the computer with the file.
- Certain approval methods, such as approving a publisher, make all instances of a file locally approved. These are not discussed in this section. See [“Approving or Banning by Publisher”](#) on page 236 for details of how publisher approvals affect file state.
- You must have full Suite licenses (Visibility and Control) to be able to reassign a computer to Local Approval policy; sites with only Visibility licenses cannot perform the reassignment.

## Automatic Local Approval on Enforcement Level Change

Bit9 security policies have an Advanced Setting, enabled by default, that causes unapproved files discovered while Bit9 Agent is in a policy whose Enforcement Level is Low or None (Visibility) to be locally approved when the policy makes a transition to Medium or High Enforcement.

Automatic local approval of unapproved files allows you to install new files while in Low Enforcement and then change to a more restrictive Enforcement Level without restricting the execution of the files that existed at the time of transition. Files that you explicitly ban remain banned, and unapproved files discovered while in Medium or High Enforcement remain unapproved during transitions to and from any Enforcement Levels.

You can disable this feature if you choose, on a policy-by-policy basis. This will increase security against unwanted execution of unapproved files already on an agent before the

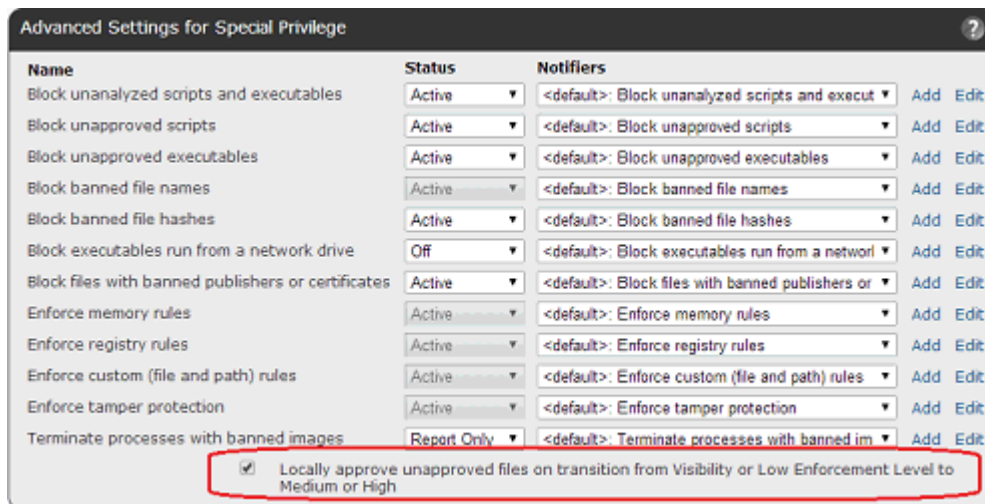
transition, but it might also cause more blocks of non-risky software after the transition. If you do not plan to enable automatic local approval, consider other bulk approval methods that might reduce the number of individual files you must approve.

**Note**

Enforcement level changes can happen because a computer changes policy or because the enforcement level of the policy itself changes. If a computer changes policy, it is the setting in the *policy it begins in*, not the policy it changes to, that determines whether the approval-on-transition takes place.

**To disable automatic local approval of unapproved files on Enforcement Level change:**

1. On the console menu, choose **Rules > Policies**. The Policies page appears.
2. Click the View Details (pencil) button next to the name of the policy you want to change. The Edit Policy page for that policy appears.
3. Click the **Show Advanced Settings** button. The Advanced Settings panel appears.



4. At the bottom of the Advanced Settings panel, un-check the *Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High* checkbox.
5. Click the **Save** button.
6. Repeat steps 2-5 for any other policies you want to change.

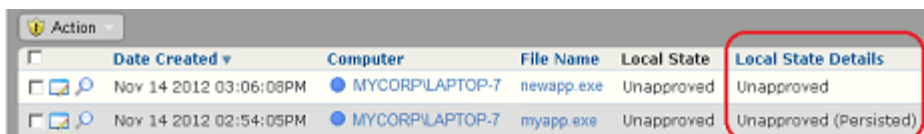
You can re-enable automatic local approval by checking the checkbox.

## Which Files Are Locally Approved On Transition

There are two types of locally “unapproved” files, and these have different Local State Details:

- Files with Local State Details of *Unapproved* were discovered on a system in None (Visibility) or Low enforcement. They will be locally approved by a change to Medium or High Enforcement Level.
- Files with Local State Details of *Unapproved (Persisted)* were discovered on a system in Medium or High enforcement. They remain Unapproved on transition.

You can view Local State Details on the Files page or Find File results (for multiple files) or the File Instance Details page (for one file). In any of the tables, add the *Local State Details* column if it is not shown.



Action	Date Created	Computer	File Name	Local State	Local State Details
	Nov 14 2012 03:06:08PM	MYCORP\LAPTOP-7	newapp.exe	Unapproved	Unapproved
	Nov 14 2012 02:54:05PM	MYCORP\LAPTOP-7	myapp.exe	Unapproved	Unapproved (Persisted)

For one policy, the Related Views menu on the Edit Policy page includes an **Unapproved files from computers in this policy** link that opens the Find Files page with the results of a file search for these files. Viewing this list may be useful before taking actions affecting local approval of unapproved files.

## Locally Approving Individual Files

You might discover that one or more files you thought were present during Bit9 Agent initialization were missing, and as a result, those files are not locally approved. A missing file could be a standalone executable or a file whose absence prevents an application from running. If you can identify the missing files and put them on the computer, you can locally approve them on an instance-by-instance basis.

You can do local approvals from any console table that shows file instances, including:

- the Files on Computers tab on the Files page, which shows instances of tracked files on every agent-managed computer on your network
- any file view of a Baseline Drift Report Results page
- the Find Files page when you have search results displayed

### Note

If you are looking for a particular file on one computer, you can add a Computer filter to your Find Files query and enter the computer’s name. The resulting search will find the file you are looking for only on the computer you entered.

You can use filters on any of these pages to get exactly the list of files you want, or one particular file.

**To locally approve individual file instances from a table of files:**

1. Locate the file instance(s) you want to locally approve in the file table.
2. In the table, check the box to the left of each file instance you want to locally approve. Confirm that the computer name next to each file is a computer you want to affect.
3. On the Action menu, choose **Approve Locally**. The Local State of each checked file becomes *Locally Approved* for the computer on which it appeared.

**Note**

To get more information about a file before you locally approve it, click on the View Details (pencil) button in the file table to bring up the File Instance Details page. That page also includes an **Approve Locally** choice on the Actions menu if the file is not already globally or locally approved.

## Removing Local Approval

Just as you can locally approve an individual file, you can *remove* local approval on a file that has been locally approved. You might choose to do this if a file you really didn't want approved happened to be on a computer at Bit9 Agent initialization, or if you mistakenly approved the file by one of the post-initialization methods. You locate the file or files the same way you would if you wanted to approve them, and then do one of the following:

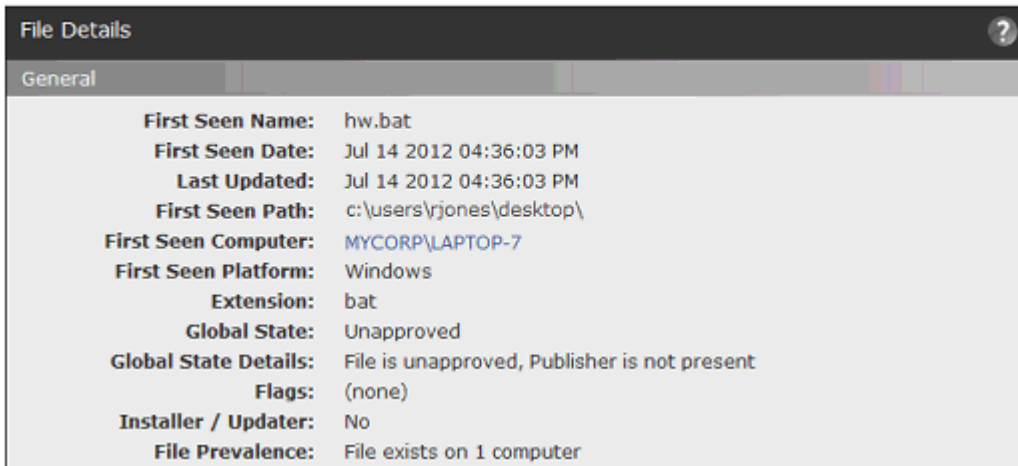
- In a file table (Files page, Find Files page, Baseline Drift Report Results), check the box next to each file whose local approval you want to remove and choose **Remove Local Approval** on the Action menu.
- On a File Instance Details page, click the **Remove Local Approval** link.

## Locally Approving Files Not Yet in File Catalog Inventory

As new files are discovered by agents, the addition of file instances to the server is processed in the background to allow efficient operation of the server and console. Because of this, the Events page might report that a new file has been discovered on a computer before that file actually appears as a file instance in the Files on Computers page.

You can locally approve a file from the Events page by choosing Approve Locally from the Action menu on the page. You also can click on the highlighted file path in the Event Description to go to the File Details page. If you do this for a file that is not fully processed, you see a note at the top of the File Details page.

**Note:** Specific file instance cannot be found - file might have been deleted or have not been processed yet. Note that computer MYCORP\LAPTOP-7 still has 35 files to process. Displaying global file details.



You can use the Approve Locally command from the Actions menu on the File Details page even though file was not found.

## Locally Approving Transient or Deleted Files

There may be cases in which a file appears briefly on a computer to accomplish a particular task. One example of this is a printer driver installation, during which a temporary file could appear long enough to install the driver and then disappear. Although this file does not appear in the Files on Computers page, you might want to locally approve it by hash so that installation of this driver is not blocked by Bit9 on a particular computer.

As with files that are present on an agent computer but not fully inventoried, you can locally approve transient or deleted files through the Action menu on the Events page or the Actions menu on the File Details page for the file. This local approval persists for all instances of this file that appear on the same computer in the future, even after the instances are deleted.

### Note

You cannot *remove* local approval of files that do not currently exist on a computer.

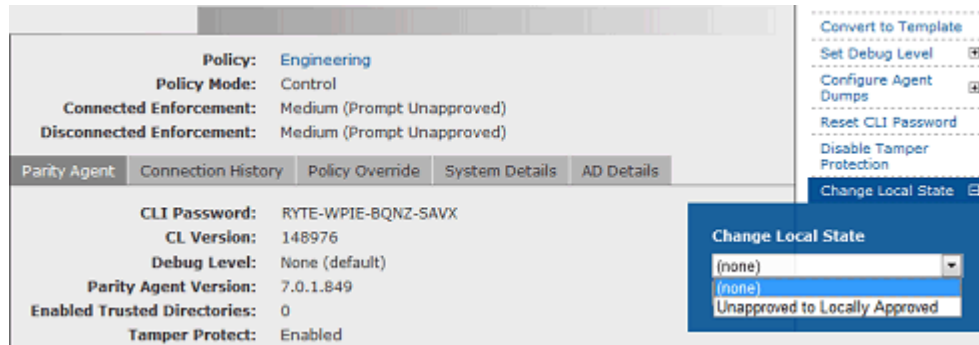
## Locally Approving All Unapproved Files on a Computer

The Bit9 Security Platform provides a mechanism for locally approving all unapproved files on a selected computer. You might choose to do this if you have added a large number of known-good files to a computer after initialization, at which point they are in the unapproved state (if not explicitly banned or globally approved).

### To change all unapproved files on a computer to Locally Approved:

1. On the console menu, choose **Assets > Computers**.
2. Click the name of the computer whose unapproved files you want to convert. The Computer Details page for that computer appears.

3. In the Advanced menu on the lower right of the page, click on **Change Local State**, choose **Unapproved to Locally Approved** in the *Change Local States* menu, and then click the **Go** button. All files whose local state on the computer was *Unapproved* are now *Locally Approved*.



## Moving Computers to Local Approval Mode

### Note

You must have full Suite licenses (Visibility and Control) to be able to reassign a computer to Local Approval mode; sites with only Visibility licenses cannot perform the reassignment.

To permit installation of new applications on a selected computer under High Enforcement Level, you may temporarily relax protection and give the computer permission to execute any files that are not banned. Your choice of how to do this depends upon whether the computer is connected to or disconnected from the Bit9 Server:

- **For an online computer**, you can use the Bit9 Console to move the computer into another Enforcement Level for as long as it takes to complete software installation and then move it back when you are finished. This option is described in the section [“Moving Online Computers into Local Approval Mode”](#) on page 259.
- **For an offline computer**, you can use the Bit9 Console to generate a system-specific password for use on the computer to move it into another Enforcement Level for a specified time period. This option is described in the section [“Using Timed Policy Overrides”](#) on page 262.

In either case, Local Approval mode should be temporary – it has a specified time limit for the Timed Enforcement Level override, but must be returned manually for online computers, as described in [“Restoring Online Computers from Local Approval Mode”](#) on page 261.

Once you return the computer to its original Enforcement Level, all files that were in the Unapproved state before the computer was placed in local-approval mode *and were not executed while in local-approval mode* remain unapproved. Formerly Unapproved files that were run or installed while the computer was in local approval mode are locally approved on the computer but continue to have a *global* state of Unapproved.

You can move into Local Approval from both High and Medium Enforcement Level. Although you can execute unapproved files in Medium Enforcement, by using Local

Approval you eliminate the need to respond to notifiers when you attempt to run unapproved files.

## Moving Online Computers into Local Approval Mode

Local Approval mode allows you to install new files that will become locally approved without affecting the local state of any files already on the computer before the mode change or installed after the computer is returned to its normal policy. It is most useful if you have not yet introduced the new files you want to install on a computer.

You can use the Bit9 Console to move an *online* computer into the predefined Local Approval policy for as long as it takes to complete software installation. While in the local approval policy, computer users are permitted to install and run unapproved applications that were previously blocked because of High or Medium Enforcement Level, although banned files remain banned and blocked from running.

After the installation is complete, you can (and should) restore the computer to its original policy, at which point it continues to be able to run all files that were installed and locally approved while it was at the relaxed Enforcement Level.

### Notes

- Unapproved software can be installed on computers in a Low Enforcement Level policy. However, you still might want to move the computer into Local Approval to approve known-good files, especially if you might move the computer to a higher Enforcement Level at a later time.
- In Local Approval, the only active Device Control settings are *Block writes to banned removable devices* and *Block executes from banned removable devices*. All others are set to *Off*.

You can move computers into Local Approval mode in several different ways, each of which also allows you to restore the computer to its previous policy:

- You can move one or more computers at a time to Local Approval mode via the Computers page.
- You can move a single computer from High or Medium Enforcement into Local Approval using the Action menu on its Computer Details page.
- You can move a single computer into Local Approval mode using the Change Policy portlet on the console Home Page (or any other dashboard it is on).

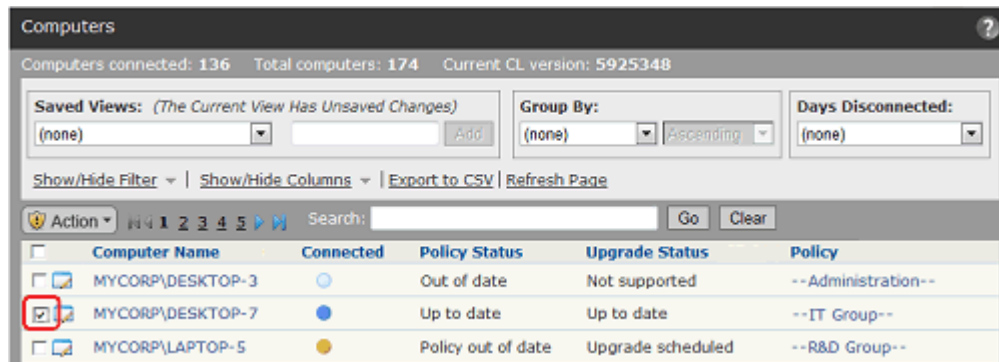
Local Approval mode has a number of special features for monitoring and control:

- You can track which machines are in Local Approval mode by choosing the Saved View *Computers in Local Approval* on the Computers page.
- You can set an alert to trigger if a computer is in Local Approval longer than a time interval you specify. See [“Using Bit9 Alerts”](#) on page 494 for more details.
- Computers manually moved to Local Approval mode can be easily returned to their normal Enforcement Level using the *Restore to Normal Enforcement Level* command on the Computers page Action menu.



**To place one or more online computers in Local Approval mode:**

1. In the console menu, choose **Assets > Computers**. The Computers Page appears.
2. In the Computers table, locate the computer to be placed in local approval mode. To reduce the number of computers displayed, you can use the Show/Hide Filters button and filter on policy or some other relevant field. You also can enter all or part of the computer name in the Search box.
3. Check the names of any computers you want to move to Local Approval mode.

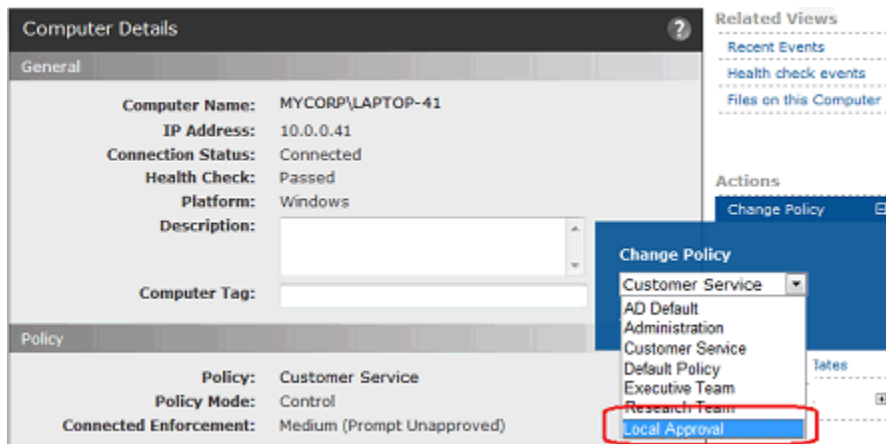


4. On the Action menu, choose **Move to Local Approval**. The computer(s) moves into the Local Approval policy. Unapproved files may be executed and device control is disabled except for writing to banned devices, which is blocked. Note that if computers in Low Enforcement are included in your selection, the operation will fail and show an error message.
5. On the Computers Page, choose **Computers in Local Approval** on the Saved Views menu. Verify that the computer appears in the table as part of the Local Approval policy. If so, the computer user may now install software on that system and have it locally approved (if not globally banned or approved). The only active Device Control setting is *Block writes to banned removable devices*.

**To move one online computer to Local Approval mode (Computer Details page):**

1. On any page displaying a Computer Name field, click on the name. The Computer Details page for that computer appears.
2. In the Actions menu, click on **Change Policy**. The Change Policy dialog appears
3. On the Change Policy menu, select **Local Approval** and then click the **Go** button. The computer moves into the Local Approval policy. Unapproved files may be executed and the only active Device Control settings will block writes to and execute attempts on removable devices. (Local Approval appears on the menu only for computers in High and Medium Enforcement.)





4. On the Computer Details page, confirm that the Policy has changed to Local Approval. If so, the computer user may now install software on that system and have it locally approved (if not globally banned or approved).

## Restoring Online Computers from Local Approval Mode

When you have put computers into Local Approval mode, you normally should restore them to their previous policy as soon as possible, after you have finished installing new application(s) on them. As with the transition to Local Approval, restoration to the previous policy can be accomplished from the Change Policy portlet, the Computer Details page, or the Computers page. The last of these is described here.

### Note

The method described below works only for online computers. If you used a timed Enforcement Level override to move an offline computer into Local Approval mode, the computer will move back to its normal Enforcement Level automatically when the time period is over. See [“Using Timed Policy Overrides”](#) on page 262 for more information on that case.

### To restore Local Approval mode computers to their previous policy:

1. In the Console menu, choose **Assets > Computers**. The Computers page appears.
2. On the Computers page, choose **Computers in Local Approval** on the Saved Views menu and verify that the computer appears in the Local Approval policy.
3. In the table, check the box next to the computer you want to restore. If you have multiple computers to restore, select each one.
4. On the Action menu, choose **Restore to Normal Enforcement Level**. The computer moves back to its previous policy. It should no longer be displayed in the Computers in Local Approval view.

## Using Timed Policy Overrides

You might need to install new applications on a selected computer under High Enforcement Level protection. You can do this by temporarily relaxing protection and giving the computer permission to execute any files that are not banned; that is, you move the computer into the predefined Local Approval policy for as long as it takes to complete software installation.

Because disconnected computers cannot be controlled directly from the Bit9 Server, you need a different way to instruct the agent to make the transition to another Enforcement Level. You can generate a special code that can be entered on a agent-managed computer to switch its Enforcement Level for a specified amount of time. The code is specific to one agent, and it can be used only once. You can generate codes to switch a computer into any Enforcement Level except *None (Disabled)*, although this feature is primarily intended for temporary transitions to Local Approval mode.

You can specify a duration of up to 500 minutes for the Enforcement Level change.

Once the specified time for the override has elapsed, the computer is automatically restored to its original policy. If you had moved it temporarily into Local Approval, it continues to be able to run all files that were installed while it was in Local Approval. Files run or installed while the computer was in the Local Approval policy are locally approved on the computer (unless globally banned or banned for that computer's policy) but continue to have a *global* state of unapproved.

While especially convenient for disconnected computers, a timed policy override may be used for a connected computer. The override procedure disconnects the agent during the override. On Mac and Linux computers, the override is maintained until the designated time period expires, even if the agent or computer is restarted during this period.

**Platform Note:** Use of timed overrides is *not* recommended for Windows computers that are currently connected to Bit9 Server. If a Windows computer or agent is restarted during the timed override, the override is ended. If you were using the override to install and locally approve an application, this could interrupt the installation and prevent approval of some necessary files, making the application unusable. To avoid unexpected results, Windows clients should be physically disconnected from the Bit9 Server when using timed Enforcement Level overrides.

### Caution

If you use a Temporary Policy Override Code to switch a computer's Enforcement Level to *Low* or *None (Visibility Only)*, when the agent transitions back to its original Enforcement Level, it might locally approve certain unapproved files discovered on that computer while in the more relaxed Enforcement Level – this affects files with Local State Details of *Unapproved*, and depends on whether *Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High* is checked in the Advanced Settings for the policy that computer is assigned to. Bit9 recommends that unless you are certain that this automatic local approval setting is **off**, you only use the Enforcement Level override feature for temporary transitions to *Local Approval*, *Medium*, or *High Enforcement*.

**To generate a code to place a computer in temporary local approval mode:**

1. On the console menu, choose **Assets > Computers**. The Computers page appears:

Computer Name	Days Offline	Connected Enforcement	Disconnected Enforcement	Policy
MYCORP\Laptop-3	1 day(s)	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	--Sales--
MYCORP\Terminal-4	2 days(s)	High (Block Unapproved)	High (Block Unapproved)	--POS Devices--
MYCORP\Terminal-2	2 days(s)	High (Block Unapproved)	High (Block Unapproved)	--POS Devices--
MYCORP\Laptop-34	2 week(s)	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	--Sales--
MYCORP\Laptop-67	5 day(s)	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	--Sales--

2. In the table, locate the computer for which you want to generate a code and click on its name. The Computer Details page for that system appears.
3. Click the **Policy Override** tab in the panel at the bottom of the page.

Temporary Enforcement: Local Approval  
 Enforcement Level Active For: 30 Minute(s) (up to 500)  
 Key Valid For: 5 Minute(s)  
 Generate Code

4. In the Temporary Policy Override Code panel, unless you want to transition to a different Enforcement Level, leave the default choice for *Temporary Enforcement*, which is **Local Approval**.
5. In the *Enforcement Level Active For* box, enter the number of minutes (up to 500) you want the Enforcement Level change to last.
6. In the *Key Valid For* box, enter the length of time you want the override code to be valid. Your choice for this field should take into account how long it will take to get the key to the computer user who needs it and how quickly they will be able to enter it.
7. When you have entered all parameters, click the **Generate Code** button. A code consisting of nine sets of letters separated by dashes appears in the box next to the button.

Temporary Enforcement: Local Approval  
 Enforcement Level Active For: 30 Minute(s) (up to 500)  
 Key Valid For: 5 Minute(s)  
 Generate Code: CARS-TALK-BLUE-LEE-LOUD-ONE-FALL-HOLD-TIN  
 This code will be valid until Feb 3 2012 15:30

8. Copy and save the code from the box (and note the computer name) so that you can deliver it to the person who will be installing new software on the offline computer. The code is *not* saved on the Computer Details page, so you must record it.

The procedure for applying the override code depends on the platform (Windows, Mac, Linux) of the agent computer.

### Overrides on Windows Agents

On Windows computers, disconnecting the agent from Bit9 Server is strongly recommended before initiating an override.

#### To use a Timed Policy Override code on a Windows computer:

1. On the offline computer, locate and run the program **TimedOverride.exe**, which is in the Bit9 Agent installation directory. An authorization dialog box appears.
2. Enter the override code for this agent into the dialog box and click **OK**.
  - If the code entered is invalid or expired, or if TimedOverride.exe is unable to communicate with the Bit9 Agent for any reason, an error message will be displayed. After three invalid attempts, the program automatically closes.
  - If a valid code is entered and the Enforcement Level transition is successful, no message is displayed but the dialog box closes.
3. If there was no error code and the dialog box is no longer displayed, you can begin installing the new software needed on this machine (assuming your override code was for Local Approval). The Enforcement Level will return to its original Enforcement Level after the time period configured when the code was generated.

### Overrides on Mac and Linux Agents

On Mac and Linux computers, it is not necessary to be disconnected from Bit9 Server before initiating an override. If the agent is connected to Bit9 Server, the override procedure automatically disconnects it and then reconnects it after the override period is over. Machine reboots or agent restarts do not cancel the timed override.

On Mac and Linux computers, you use the override code in special agent management commands to apply a timed policy override.

#### To use a Timed Policy Override code on a Mac and Linux computer:

1. On the computer you want to apply the override to, open a terminal window and change to the following directory:
  - On Linux, `cd /opt/Bit9/bin`
  - On Mac, `cd /Applications/Bit9/Tools`
2. Enter the following command with the override code you generated as an argument:  
`./b9cli -timedoverride <code>`
  - If the code entered is invalid or expired, an error message will be displayed. After three invalid attempts, the program locks out further attempts for an hour or until the agent is restarted.
  - If a valid code is entered and the Enforcement Level transition is successful, the message *Timed override set* is displayed.

3. When the override is set, the agent is disconnected from the server (if connected) and you can begin installing the new software needed on this machine (assuming your override code was for Local Approval).

The Enforcement Level will return to its previous setting after the configured override period expires. On Mac and Linux computers, if the computer was connected when the override code was applied, it is reconnected to its Bit9 Server. When reconnected (whether immediately or at a later time), the agent reports events associated with the Enforcement Level change to the server.

## Marking a File as an Installer/Not an Installer

When it analyzes a file, the Bit9 Security Platform determines whether the file is likely to be an *installer* – that is, whether it will generate additional files when executed. By locally approving a file identified as an installer, you make any files it installs locally approved as well. Files not identified as installers do not transfer their approval status to files they generate, if any.

It is possible that a file is mis-categorized, or that you prefer not to have the local approval of a top-level file cause local approval of the files it installs. You can override installer status in both directions using menus on the file details pages. For each file, you see only the menu choice that reverses the current status.

### Note

For this release, no Linux files are recognized as installers. The only Mac files recognized as installers are packages – files with .PKG extensions and properly defined *archive* headers. Because of this, using the *Mark as installer* feature might be particularly useful for this platforms.

### To mark a file as an installer:

- On the File Details or File Instance Details page, click **Mark as Installer** in the Actions menu.

### To mark a file as not an installer:

- On the File Details or File Instance Details page, click **Mark as Not Installer** in the Actions menu.

### Notes

- When you override the installer status of a file, that override is shown in the Local State Details for the file.
- In file tables, if you check the box next to a file *not* identified as an installer, and you choose Approve by Policy on the Action menu, you can mark the file as an installer as part of your approval rule. This ensures that new files it writes will be locally approved. Files it has already written will remain in their current state.
- You can create a Custom Rule that *Promotes* files meeting the rule specifications. This treats these files as installers under the conditions of the rule but does not change their global status as an installer or not an installer. See [Chapter 12, “Custom Software Rules.”](#)

## File-Specific Rules: Approvals and Bans

The Files tab of the Software Rules page shows all of the approvals and bans created at your site for specific individual files. These rules identify specific files by hash or optionally by file name (for bans only).

Approvals and bans can be global, applying to all computers, or they can be applied to computers in selected policies. Active Bans block file executions for affected computers in Control mode, report an event for computers in Visibility mode, and do nothing for computers in Agent Disabled mode. You also can create a Ban that only reports what it would have done if active.

Because the Files tab shows both Approvals and Bans, you can manage all file rules in one place. You can check to see whether a particular file has any approval or ban affecting it, and you can remove rules from one or more checked files.

Software Rules: File Approvals and Bans

Updateers Publishers Users Directories **Files** Custom Memory Registry Scripts Reputation

Group By: Type Ascending

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Add File Rule Import Delete File Rule

Type	Name	File or Hash	Is Global	Source	Last Modified By
<b>Type: Approval</b> 5 items					
Approval	updater	82E63...2609C (SHA-256)	Yes	Manual	admin
Approval	File Utility	57F33...915D3 (SHA-256)	Yes	Manual	admin
Approval	XYZ Installer	561DC...F88EA (SHA-256)	Yes	Manual	admin
Approval	abcd.tmp	73F7E...14886 (SHA-256)	Yes	Trusted Directory	System
Approval	mydll.dll	F6E34...5737F (SHA-256)	Yes	Trusted Directory	System
<b>Type: Ban</b> 3 items					
Ban	afile.sys	E38F2...EF04E (SHA-256)	Yes	Manual	admin
Ban	kazaa_setup.exe	*kazaa_setup.exe	Yes	Manual	admin
Ban	badfile.exe	2FB66...C3AC6 (SHA-1)	Yes	Manual	admin
<b>Type: Ban (Report Only)</b> 1 item					

9 items in 3 groups Page 1/1 25 rows per page

By default, file rules are grouped by their *type*, so you see all of the Approvals together, Bans together, and Report Only bans together. As with most console tables, you can change (or eliminate) the grouping by making another choice on the *Group by* menu.

You can create approvals and bans directly on the Software Rules page Files tab if you want to enter the file hash or name manually in a property page. The easier way to create bans, however, is from a table or File Details page that already has the file hash in it. In either case, when you create the approval or ban, it appears on this page.

When you create a new ban or approval, it might affect a file that already has an approval or ban. If you attempt to do this, a warning appears, informing you that if you save the new rule it will delete the old rule. This can be especially helpful if you select a group of files and are accidentally replacing a ban with an approval on some files, or vice versa.

In some cases, creating a ban not only prevents future executions of a file but stops any currently running processes matching that file. See [“Enabling Bans to Stop Running Processes”](#) on page 279 for more details.

### Note

Approvals and bans on the Files tab are rules created specifically for a given file (by name or by hash). This page does not show *all* approvals or bans that take effect because of other rules, including Reputation and Custom Rules, and it is not a comprehensive list of global *file state*. If you want to see all files whose *global state* is approved, use the File Catalog.

Approvals and bans that appear on the File Rules page are created in the following ways:

- From the Software Rules Files tab, open the Add File Rule page and enter the hash for a single file; for bans, you also have the option of using the file name or a specific path
- From a File Details or File Instance Details page, choose one of the approval or ban commands on the Actions menu to create a rule for a single file.
- In a table of files (e.g., the File Catalog), check one or more files and choose one of the approval or ban commands on the Action menu to create one or more rules.
- In the Events table, check one or more events that have a file reference in the description and choose one of the approval or ban commands on the Action menu to create one or more rules.
- From the Software Rules Files tab, import a list of file hashes to create multiple rules.
- From the Software Rules Directories tab, create a Trusted Directory. Each file located in a trusted directory has an approval rule created for it.
- An approval or ban might be created through an external API. Rule origin also might be unknown, for example if the rule was created in an older version of the Bit9 Security Platform (Parity). The *Source* field on the Files tab or Edit File Rule page shows how a rule was created.

Once you create a rule, you can manage it from the File Rules page, and in most cases you can delete it using commands on the page you used to create it.

### Caution

Banning the wrong file can have unintended and possibly harmful consequences. For example, inadvertently banning a legitimate system file could cause computers to immediately crash. Before you ban a file, ensure that you enter the correct name or hash. As a precaution, first search the file name or hash with the Find Files feature to verify that it is the file you want to ban, and review the File Details page. For further assurance, consider using Bit9 Software Reputation Service (SRS) to learn more about the file before banning it. For more information, see [Activating Bit9 SRS in Chapter 23, “System Configuration.”](#)

One way to test the impact of a ban without actually blocking files is to create a Report Only ban.

Testing a ban through Report only is especially advisable if you have enabled termination of running processes when bans are created. See [“Enabling Bans to Stop Running Processes”](#) on page 279.

### Report Only Bans

Creating a *Ban (Report Only)* rule enables you to observe how a ban might affect your users. With a report-only ban, the file is not blocked but *would-have-blocked* and *would-have-terminated* warnings are written to the Events log. If you are certain this is a file you want to block from executing, you can change the rule to a full Ban. See [“Event Reports”](#) on page 482 for more information about Bit9 event reporting.



## Creating an Approval or Ban from the Software Rules Page

If you want to specify all of the parameters for an approval or ban, you can create it on the Add File Rule page.

**To create and configure an approval or ban for a single file:**

1. On the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click the **Files** tab. The File Approvals and Bans table appears:
3. Click the **Add File Rule** button. The Add File Rule page appears, with Approval as the default Rule Type:

4. Specify the information about the rule and the file to be approved or banned (Table 39 shows the full list of possible parameters as well as rule information available after creation):
  - a. Provide a Rule Name so that you can identify the rule in the table.
  - b. Choose the Rule Type (*Approval, Ban, Ban (Report Only)*). Note that if you choose Ban, a warning appears stating that the Ban could stop matching files currently running. See “[Enabling Bans to Stop Running Processes](#)” on page 279 for details.
  - c. If the rule is a Ban, choose the Type (*Hash or File Name*).
  - d. For Hash rules, specify the type of hash you will provide (*MD5, SHA-1 or SHA-256*).
  - e. For FileName Bans, choose the platform to which the rule will apply (*Windows, Mac, or Linux*).
  - f. Enter the Hash Value or File Name that will identify the file.
  - g. Optionally, provide a Description.
  - h. In the Rule Applies To field, choose *All policies* or specify the *Selected policies* to which the rule will apply.
5. To create the approval or ban, click **Save**. The rule appears on the File Rules table. Group the table by Type (the default) if you want to see Bans together, Report Only bans together, and Approvals together.

When you save a rule, the parameters that define the rule and additional information about it are available on its details page. Table 39 shows the information that appears on the Edit

File Rule page. Which fields on the page are editable depends upon how the rule was created.

**Table 39:** File Rule Parameters

Field	Description
<b>Rule Name</b>	Text description of the files to be approved or banned. This could be a file name or other identifying information to help you manage the rule (the rule is created even if you do not enter a name). <b>Note:</b> This is name for the rule only. Entering a file name here does not create a filename-based rule.
<b>Rule Type</b>	The choices are Approval, Ban, and Ban (Report Only), which reports events for situations in which the file would have been blocked if the rule had been a full Ban.
<b>Source</b> (Read Only)	How the rule was created. The possible values are: Manual (created from scratch or from Action menu commands), Trusted Directory, Imported (from an uploaded list of files), External (API), and Unknown. Appears after the rule is created.
<b>Type</b> (Bans Only)	To ban a file you must know the Name of the file or its Hash (data signature). Choose one, as appropriate. If you choose Name, you can enter a path so that the rule only applies to a file in a particular location. Approvals are always by hash, so the Type field does not appear for them. Name bans must be platform-specific.
<b>File Name</b> (Bans Only)	(Appears only for bans, and only if you chose File Name as Type) Name of the file and its extension. For example, msblast.exe. Specify a directory path if you want to ban only matching files in a particular location. If you use a path, files with the same name that appear in any other directory are not subject to the name ban. <b>Platform Note:</b> If you enter a path, be sure to use the correct directory delimiters, and to use only characters and formats legal for paths in the chosen platform. The Bit9 Server does not convert paths between platforms (e.g., \ to /). Also, Linux file names normally are case sensitive.
<b>Platform</b> (Ban by Name Only)	(Appears only for bans, and only if you chose File Name as Type) Platform for which this rule is effective (Mac, Linux, Windows). Name bans must be platform-specific.
<b>Hash Type</b>	Cipher algorithm used to create the hash you want to approve or ban. If you paste in a value, the choices are MD5, SHA-1, and SHA-256. Rules created from a file table or details page use SHA-256, if available.
<b>Hash Value</b>	Hash (data signature) for the file. Hashes not yet seen by this Bit9 Server can be used in rules. To locate hashes for files already found on your computers, you can use the File Catalog or Find Files pages.
<b>Description</b>	Optional text to further describe the file approval or ban. This information is displayed in File Rules table under the Description column (if visible).

Field	Description
<b>Rule Applies To</b>	<p>Policies for which the approval will be enforced:</p> <p>Select <b>All policies</b> to approve or ban the file for all computers.</p> <p>Select <b>Specified policies</b> to choose which policies to apply the rule. When you click this button, a list of policies appears, each with a checkbox. You also can use the checkbox at the top of the list to check all boxes or clear all checks, but keep in mind that you cannot create a rule that applies to no policies.</p>
<b>History</b> (Read Only)	<p>Shows when and by whom the rule was created and last changed. Also shows the CL version (i.e., the version of Bit9 rules) in which the current version of the rule is present, which can be used to determine whether the rule is present on an agent.</p>

## Editing and Deleting File Rules

You can modify or delete an existing File rule. In [Table 39, “File Rule Parameters”](#) on page 270, some of the parameters can be changed and some are read-only.

### To edit an approval or ban rule:

1. On the Files tab of the Software Rules page, click the View Details (pencil and file) button next to the rule. The Edit File Rule page appears.
2. Edit the details you want to change. You can change all rule parameters *except for* Type (hash or file), Hash Type, and Hash Value. Also Source and History are read-only fields added to the page to reflect activities related to the rule.
3. When you have finished making changes, click **Save**. The rule is updated.

### Note

You cannot disable an existing approval or ban. You can, however, change the Rule Type. For example, you can change a ban from an active ban to Report Only, which will prevent it from blocking but still report file executions it would have blocked.

You also can change a Ban to an Approval or vice versa, but be certain you understand the effects before doing this. If you don't want a rule enabled in any way, you must delete it.

To delete a File rule, you can use the **Remove Approval or Ban** commands on the Action menu of any file table page, or the appropriate *Remove* command on a details page. If you are on the Software Rules page Files tab, you delete rules using the following procedure.

### To delete one or more approval or ban rules:

1. On the Files tab of the Software Rules page, check the box next to the approvals and bans you want to delete.
2. Click the **Delete File Rule** button.
3. In the confirmation dialog box, click **OK**. The rules are removed.

You also can delete a single approval or ban by clicking the **Remove Rule** button on its Edit Rule page.

## Creating File Approvals and Bans from Table Pages

The following procedure describes creating an approval or ban rule from the Files page (File Catalog or Files on Computers), but it applies to any other console page that lists files as well as pages in which the file is not the primary information but might be included as a link in details of another object. Generally, a row with a checkbox next to a filename allows creation of bans and approvals from the Action menu. This includes:

- Files page (both File Catalog and Files on Computers)
- Baseline Drift Report Results pages that list files
- Snapshot Content page
- Events page (only events that include file hashes)
- Find Files page (when showing results)

The Action menu provides the following choices for managing approvals and bans from a tables page:

- **Approve Globally** – Immediately creates a hash-based rule globally approving a file for all computers – no configuration is necessary.
- **Ban Globally** – Immediately creates an active hash ban applying to all computers and operating – no configuration is necessary.
- **Approve by Policy** – Opens the Add Rule page with the file name as Rule Name, Approval as the Rule Type, and the file Hash already in place. You can choose to apply the rule to selected policies or all computers and, you can edit the rule name and add a description.
- **Ban by Policy** – Opens the Add Rule page with the file name as Rule Name, Ban as the Rule Type, and the file Hash already in place. You can choose to apply the rule to selected policies or all computers, you can edit the rule name and add a description, and you can make the rule an active ban or just a report-only ban.
- **Remove Approval or Ban** – Immediately removes the rules for all checked boxes, including mixed selections of approvals and bans.

The advantage of creating an approval or ban from a console files table is that you can approve or ban multiple files at once. For example, you might use the filtering tools on a files page to get a list of files meeting certain criteria, check the box next to each file's name, and globally ban them in one operation.

First Seen Name	Publisher or Company	Product Name	Trust	Global State
10:25AM googleupdatesetup.exe	Google Inc.	Google Update	10	Unapproved
5:34PM solsuite.exe	TreeCardGames.com		8	Unapproved
8:24AM crashreporter.exe	Mozilla Corporation	Firefox	10	Unapproved
8:24AM brwsrcomp.dll	Mozilla Corporation	Firefox	10	Unapproved
4:48AM swdir.dll	Adobe Systems Incorporated	Shockwave	10	Unapproved

When you create a rule from a table, the rule definition you provide applies to each selected file. When you save the definition, a separate rule is created and named for each selected file. Rules created from checked rows of a table are always hash bans, and use SHA-256 hashes if available.

### Notes

- Initially, files that originate from a common source or installer are grouped under the source/installer file name. If you are looking for a file to approve or ban and want to include all *individual* files grouped under an installer in the table so that you can view and search them, check the **Show Individual Files** box in the lower right corner of the Files page, which automatically refreshes the table.
- You can filter the lists of files on the Files page, rearrange display columns, and download results in comma-separated-value format. For more information, see [Bit9 Console Tables](#) in Chapter 2, “Using the Bit9 Console.”

## Creating Global Approvals and Bans

The Action menu on files pages has two shortcut commands, one of which creates a global ban and the other a global approval for the files you check on the page. These commands give you a quick way to approve or ban one or more files as long as you do not want to create any special configuration for the rules you create.

When created this way, rules apply to all policies. If you choose *Globally Approve*, checked files are globally approved for all computers and each file has a separate approval rule on the Software Rules page. Likewise, if you choose *Globally Ban*, the files are banned on all computers in Control policies and each file has a separate ban rule on the Software Rules page.

For both approvals and bans, if you checked one file, the file name is used as the rule name. If you checked more than one file, the name is left blank.

### Notes

If you select files that already have a rule and apply a different type of rule to them, it is possible that the name of the old rule will be maintained and the rule type will be changed. This could be confusing if you named a rule something like “Approve Files for My Project” and then changed the Rule Type to *Ban*.

### To create a global approval or global ban for one or more files on a Files page:

1. On the console menu, choose **Assets > Files**. The Files page appears.
2. Locate the files you want to approve or ban and check the boxes next to their names.
3. On the Action menu, choose **Globally Approve** or **Globally Ban**.
4. In the confirmation dialog box, click **OK**.

## Custom Approvals and Bans

When you choose Approve by Policy or Ban by Policy on the Action menu of a file table, an Add File Rule dialog appears with the hash(es) for the files you selected already entered. Unlike choosing one of the global options, this choice allows you to customize other parameters before you create the rule.

### To create a custom approval or ban for one or more files shown on the Files page:

1. On the console menu, choose **Assets > Files**. The Files page appears.
2. Locate the files you want to approve or ban and check the boxes next to their names.
3. On the Action menu, choose **Approve by Policy** or **Ban by Policy**. The Add File Rule page opens.

The screenshot shows the 'Add File Rule' dialog box. The 'General' tab is active. The 'Rule Type' is set to 'Approval'. The 'Hash Type' is 'SHA-256' and the 'Hash Value' is '[Multiple values]'. The 'Description' field is empty. The 'Rule Applies To' section has 'All policies' selected. The 'Installer Information' section contains the following text: 'None of the selected files have created or modified other files. 5 files of the 5 selected are not installers. Use the following option if the files you are approving should be allowed to update or create approved content: [ ] Mark all files as installers'. At the bottom are 'Save' and 'Cancel' buttons.

4. You can change the Rule Type, including changing from **Ban**, which actively blocks executions, to **Ban (Report Only)**, which just reports that the file would have been blocked if the ban was fully activated.
5. You can add an optional description of the rule (for example, something the approved files have in common or why you banned the files on them).
6. In the *Rule applies to* field:
  - a. To apply the rule to all computers, leave the *All policies* button selected.
  - b. To apply the rule to selected policies only, click the *Selected policies* button.
7. If the Rule Type is Approval, an Installer Information panel is included at the bottom of the page. If any of the files selected for approval is not currently recognized as installers, a *Mark all files as installers* checkbox appears in the panel. Check the box if you want the files to be approved and marked as installers.

**Important**

Especially when you have multiple files selected for the rule, be certain you want *all* of the files to become installers before you check the *Mark all files as installers* box. Files created by installers are locally approved, and there is no automatic way to remove this approval. The message in the Installer Information panel will tell you how many files in your selection would be affected by this choice, and whether any files in the selection have created or modified other files.

- When you have configured the rule as you want it, click the **Save** button. Each file you checked when you started the process appears on the Software Rules page Files tab as a separate approval. The File Approvals and Bans table indicates whether an approval or ban is global or not.

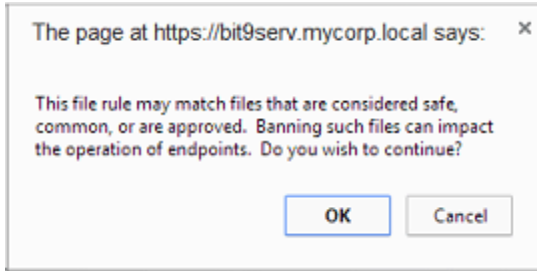
**Warnings when Creating or Editing Bans**

When you create or edit a ban, the File Rule details dialog will show a warning in red, indicating that the rule could stop currently running files. This appears as a reminder even if you have not enabled process termination in any policy.

In addition, when you add or edit a file ban and click Save on the File Rule details dialog, a confirmation dialog may provide a further warning. The warning appears if a name ban contains wildcards in the name. It also appears for both name and hash bans if the file specified in the rule has a Bit9 SRS threat level of either “0 – Clean” or “Unknown” *and* one of the following conditions is true:

- A ban specifies a file signed by Microsoft (including key system files)
- A ban specifies a file signed by another trusted publisher
- A ban specifies a file with Bit9 SRS trust levels above 7.
- A ban specifies a file that appears on more than 10% of reporting agent computers.





In each of these conditions, terminating the file or files indicated in the ban could have undesirable effects, including shutting down the computer. The default on this dialog is to allow the ban, so be sure to click on **Cancel** if you have any concern about the ban.

## Approving and Banning Files from the File Details Page

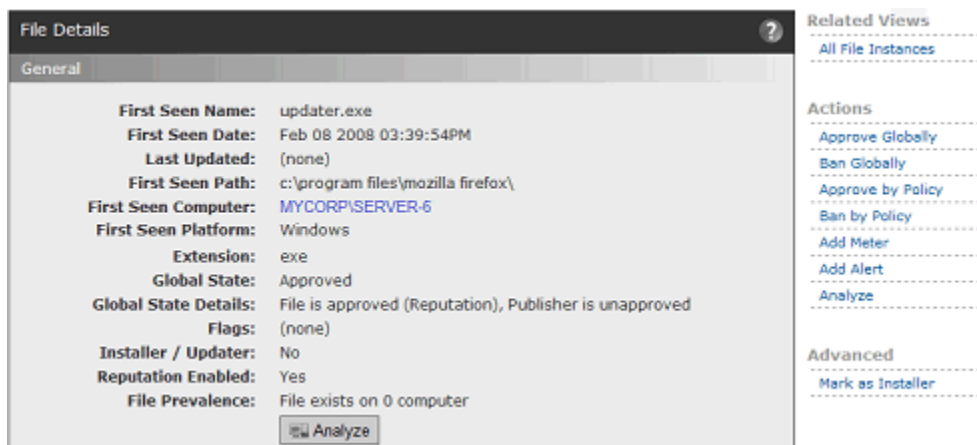
Although you can approve or ban files from tables, you might want more information about the file before you decide to ban it. For this, you can go to the File Details page.

### Note

You can follow this same procedure to approve or ban a file globally or by policy from the File *Instance* Details page, which also includes options for applying or removing local approval of an individual file.

### To approve or ban a single file using the File Details page:

1. When you find a file you want to approve or ban, click the View Details (pencil) button next to it in a table or click its hash or name if it is in the Events table. The File Details page appears (only top panel shown here):



2. Examine the information on the File Details page to be certain you want to approve or ban the file. For example, you can see in the File Prevalence line whether any computers currently have the file. To determine which computers have the file before you approve or ban it, click the **All File Instances** link on the Related Views menu.



3. If you have Bit9 SRS enabled, the Bit9 Software Reputation Service Information panel shows Trust, Threat, and other information about the file, if available. You can click the **Analyze** button to search Bit9 SRS for information if none is shown or to check for updated information.

#### Note

If you want to analyze the file but the Analyze button is not visible, see [“Activating Bit9 SRS”](#) on page 643.

4. In the Action menu, choose the rule you want to create for this file – note that if the file is already approved or banned, you must remove the current rule (using **Remove Approval** or **Remove Ban**) before you create an opposite rule.

#### Note

For more information about approving or banning hashes from the Files tab of the Software Rules page, see [“Creating an Approval or Ban from the Software Rules Page”](#) on page 269.

## Approving or Banning Lists of Files

If you have a list of hashes for files, you can import the list in a text file as input to the Bit9 Console and change their file state in one operation. You can change the file state to Approved, Banned, or Ban (Report Only), and you can do this for some or all policies.

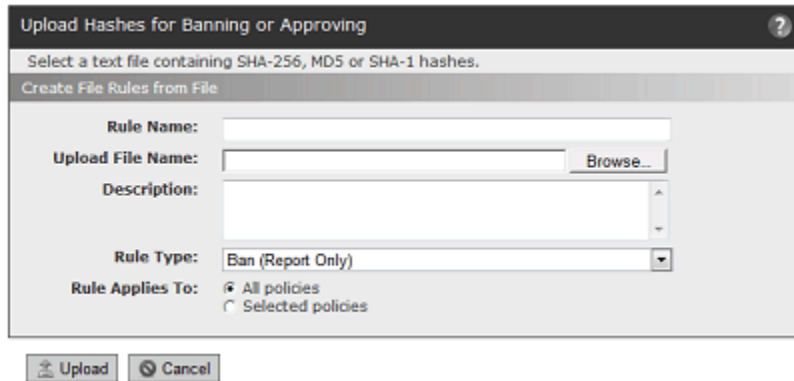
The requirements and recommendations for approving or banning lists of hashes are:

- The file containing the hash list must be accessible to the Bit9 Server.
- The file must contain a list of MD5, SHA-1, or SHA-256 hashes, with only one hash per line.
- Use only one hash *type* per file; mixing types in one file may cause unpredictable results.
- You must take the same action on all files on the list; that is, you must approve the whole list, ban the whole list, or create a report-only ban for the whole list.
- This version of the Bit9 Console is supported for Internet Explorer 10 and later. On some older versions of IE with Advanced Security Settings, you must make `https://<bit9servername>/` a trusted site in **Internet Options – Security – Trusted Sites – Sites**. Otherwise, bulk hash files cannot be processed.
- Do not navigate away from the page until the Upload Hashes page shows that the process is complete. If you do navigate away, processing of the hashes is interrupted. In this case, you can upload the file again, and any hashes not yet approved or banned will be processed.

When you use this method to approve or ban a list of files by their hashes, each file appears as a separate rule, but the rule name is the same for each.

**To create approvals or bans for a list of hashes:**

1. Copy or move the file containing the hashes to a location accessible to Bit9 Server.
2. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
3. Click the **Files** tab. The File Rules page appears with a list of Approved and Banned files.
4. Click the **Import** button. The Upload Hashes for Banning or Approving page appears.



5. Enter the rule parameters, as follows:
  - a. Enter the Rule Name as you want it to appear on the File Rules page.
  - b. Use the **Browse** button to locate the file containing the list of hashes and click **Open** in the *Choose file* dialog when you locate the file. The pathname to the file containing the hashes appears in the File name box.
  - c. (Optional) Enter a description for the rule.
  - d. Choose **Approve**, **Ban**, or **Ban (Report Only)** on the Rule Type menu.
  - e. Make the rule effective for **All policies** or **Selected policies**.
6. When you are satisfied with all of the rule parameters, click **Upload**. A two-column progress table appears as the hashes are processed, reporting the success or failure of the rule for each file and also informing you when hashes on the list are already in the state you chose.

Hash:	Status:
F98F8432D50B26B3DEF5E67BAEA0A8D7D4BA1F312940AC5CBC5D81BEFD6BA1C7	OK
BAC9967B79EF3E490B4CE23BD764693C97C47703BC4A6021FB4363DCBEB860A2	OK
5582DCLA3878C095DAAC79A1CFB006B042A6EEE4FF0B292C6FB3A5B6DC54871	OK

7. On the console menu, choose **Rules > Software Rules**. On the Files tab of the Software Rules page, the hashes you created approvals or bans for appear in separate rows in the table, but with the same Rule Name. Once rules have been created for all files on the list, each rule can be modified individually.

## Enabling Bans to Stop Running Processes

By default, file bans stop future attempts to execute a file but do not terminate processes that are already running on an agent-managed system. This means that files that are allowed to run but are later determined to be malicious will continue to run unless they are terminated for some reason other than a Bit9 rule, or if the system restarts. This is especially likely in Low and Medium Enforcement policies, where files not explicitly banned are allowed to run.

Beginning with v.7.2.0, you can configure policies so that computers in those policies stop currently running software when they receive a rule that bans it. This capability provides better control over software in your environment. It must be used carefully, however, to avoid interrupting important processes or even preventing a computer from running at all. Also, keep in mind that when enabled for a policy, process termination applies to *all* banned files. So that you can see what the effect of this setting might be, newly created policies in v7.2.0 are configured to report processes that would have been terminated by a ban, but not to actually terminate them.

### Notes

- Pre-7.2.0 agents are not affected by this feature and cannot terminate processes matching banned files.
- In Bit9 Platform v7.2.1, termination of processes with banned images is supported on Windows agents only.

Any ban, whether on a system that terminates banned processes or one that doesn't, may disrupt a user's system or cause other dependent applications to fail, possibly causing loss of work in progress. On the other hand, allowing bans to terminate running processes provides immediate feedback on the results of the ban. They also make it possible to terminate legitimate processes infected with malware and allow them to restart without the infection. The following are some examples of the potential impact of enabling process termination:

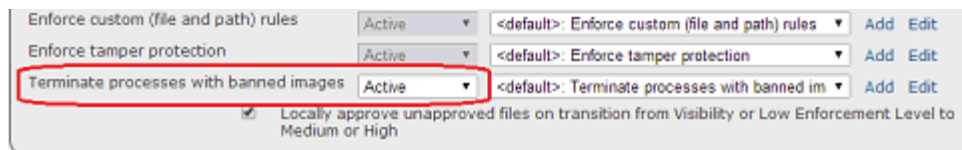
- **Discrete Single Application** – Ban skype.exe. On systems affected by the ban, all running instances of Skype are abruptly terminated and any attempt by users to restart Skype will be blocked.
- **Windows Explorer Extension** – Ban a file called malware.dll, which is registered as a Windows Explorer extension and is present in all running instances of Explorer. On systems affected by the ban, all instances of Explorer are terminated and then the Explorer is automatically restarted by Windows. On restart, the banned file malware.dll is blocked while Explorer continues to load and run, so the ban prevented the unwanted process from running without blocking the critical Explorer process. Without the terminate process setting, the unwanted process would continue to be running in every active Explorer, even after it was banned.
- **Dynamically Loaded DLL** – Ban wsock32.dll. Also assume that wsock32.dll is dynamically loaded by the application xyz.exe when it needs to perform certain network operations and then unloaded when the operation is complete. On systems affected by the ban, if the file wsock32.dll is banned while unloaded, it will be blocked the next time it is loaded by xyz.exe, likely causing the operation to fail. If the ban takes effect when the file is loaded, the process xyz.exe will be terminated.

- **Shared Service** – Ban malware.dll, which is installed as a network service and shares an instance of svchost with other running services. When the file is banned, the instance of svchost is terminated along with all services in the same process.
- **Injection in Critical Process** – Ban malware.dll, which is injected into csrss.exe, a critical system process. On systems affected by the ban, csrss.exe is terminated. Windows detects the termination of critical system processes and immediately shuts down. If the csrss.exe is reloaded again on startup, Bit9 prevents the image from being injected and allows the system to boot normally without malware being installed.
- **Boot-time Driver** – Ban malware.sys, which is installed as a boot-time driver. If the driver loads before the Bit9 Agent does, it can continue to be executed and may not be stoppable without crashing the machine. Going to safe mode to remove the infection or restore to an earlier time may be the only remediation.

Keep these and other possible effects in mind when considering whether to enable process termination in a policy.

**To enable or disable immediate termination of banned processes:**

1. On the console menu, choose **Rules > Policies**.
2. Double-click the View Details button next to a policy for which you want to configure process termination.
3. On the Edit Policy page, click the **Show Advanced Settings** button.
4. In the Advanced Settings panel for the policy, go to the last setting, *Terminate processes with banned images*. Choose one of the following items on the Status menu:
  - **Off** – Creation of a ban does not terminate or report that it would have terminated a running process.
  - **Report Only** – Creation of a ban does not terminate a running process but reports that it would have if this setting was Active.
  - **Active** – Creation of a ban terminates a running process matching the banned image.



5. Click the **Save** button above the Advanced Settings panel.
6. Repeat these steps for any other policies in which you want to change this setting.

## Chapter 9

# Reputation Approval Rules

This chapter describes reputation approval rules, which can be used to automatically approve files based on the file and publisher trust ratings provided by Bit9 Software Reputation Service (SRS).

**Notes**

Reputation approval rules require activation of Bit9 SRS. See [“Activating Bit9 SRS”](#) on page 643.

Other methods for approving files are described in [Chapter 8, “Approving and Banning Software.”](#)

**Sections**

Topic	Page
<a href="#">Overview</a>	<a href="#">282</a>
<a href="#">Reputation Approval Strategy</a>	<a href="#">283</a>
<a href="#">Creating Exceptions for Files and Publishers</a>	<a href="#">286</a>
<a href="#">Enabling Reputation Approvals</a>	<a href="#">287</a>
<a href="#">Modifying and Disabling Reputation Approvals</a>	<a href="#">289</a>
<a href="#">Views Related to Reputation Approvals</a>	<a href="#">290</a>

## Overview

Bit9 Software Reputation Service (SRS) is a cloud-based database of known files, hosted by Bit9. It pulls file data from a combination of distribution partners, Web crawlers, honeypots, and the Bit9 user community. For files in the database, Bit9 SRS provides context information such as who published the file and what product (if any) it is associated with. It also screens software using multiple anti-malware tools, and cross-references it against third-party vulnerability databases.

Using the information it has about a file, Bit9 SRS assigns a *threat* level and a *trust* rating. It also assigns a trust rating to publishers.

Reputation approval rules allow you to use these trust ratings to approve files automatically, with the following options:

- Approvals can be based on file or publisher reputation, and these options can be enabled together for maximum coverage and benefit.
- You set the trust thresholds at which you want files and publishers to be approved.
- Reputation approvals can be enabled for all agent-managed computers or by policy.
- You can disable reputation approvals for specific publishers and specific files that you don't want to be automatically approved.

If you are concerned about advanced threats, reputation approvals can be a good choice for approving files considered trustworthy. Automatic approval using reputation can give your end users more flexibility and reduce the effort of maintaining the whitelist of approved files. Note that reputation approvals are based only on a file's *trust* rating (i.e., how *safe* it is believed to be), not on whether it is appropriate for a business environment.

When you enable reputation approvals, any manual file or publisher state assignments you have made remain in effect and take precedence over reputation. For example, if you ban a file by name or hash, that file remains banned even if it would have been approved by reputation. When and how reputation approval rules affect files on computers is described later in this chapter.

## Trust Ratings for Files and Publishers

### File Trust Ratings

The Bit9 SRS bases a file's trust rating on a proprietary algorithm that takes the following factors into account:

- **Source Trust** – The origin of the file
- **Publisher Trust** – Whether the file has a signed digital certificate and the trust associated with that specific certificate
- **Malware Severity** – Whether anti-virus scanners identify the file as malicious or potentially malicious (e.g., a virus or malware); files in the Bit9 SRS database are scanned by multiple anti-virus products
- **Vulnerability Severity** – Whether there is a known vulnerability for the file (specifically, a Microsoft-reported vulnerability), and if so, how severe
- **Duration Seen** – How long this file has been seen in the field by Bit9 SRS
- **First Seen** – The date and time this file was first seen in the field by Bit9 SRS
- **Prevalence** – How common this file is in the field, as reported to Bit9 SRS

The combination of these factors is used to calculate the trust rating of a file. Bit9 SRS rates file trust on a scale from **0 (lowest trust)** to **10 (highest trust)**. For example, a signed operating system file with no known vulnerabilities would have a Trust value near 10. An unsigned third-party application not distributed via well-known websites might have a trust value of 3. Known malicious software, or an application distributing known malicious software, would have a Trust value at or near 0.

## Publisher Trust Ratings

A publisher's trust rating is based on factors including aggregate experience with files from that publisher and the publisher's general reputation. There are four possible values for publisher trust: High, Medium, Low, and Not Trusted. If a publisher is Not Trusted, either there is no information about it or it is known *not* to have any of the factors that would elevate its trust level.

## Reputation Approval Strategy

Reputation approvals allow high-trust software to run on agent-managed computers with little administrative effort. How you choose to implement reputation approvals will depend on your goals, especially the balance between convenience and protection. Although you can enable them separately, you get the maximum benefit of reputation approvals by enabling *both* file and publisher reputation approvals:

- **File reputation approvals** – Not all files are signed by a publisher. By using *file* reputation approvals, you can take advantage of the reputation data for specific files known to Bit9 SRS, regardless of whether a file has a known publisher.
- **Publisher reputation approvals** – By using *publisher* reputation approvals, you ensure that all files signed by trusted publishers, including new files that might not have their own reputation yet, are approved and can run on agent-managed computers. Files from approved publishers are approved locally on connected agent-managed computers.

You can enable reputation approvals for all computers or only for computers in specific policies. There is no performance benefit or penalty for limiting reputation approvals to certain policies, so you should enable reputation approvals for all policies except those in which you want complete control over which specific files can be executed.

### Note

When Bit9 SRS is activated, Publisher Trust values are shown on the Publishers tab. This tells you what to expect when you enable Approvals for publishers. If the Trust value for a Publisher is High, then all files from that publisher will be approved when reputation approvals for publishers are enabled.

## Setting the Trust Level for Approvals

You can set trust levels for file and publisher approvals any way you choose, but there are two recommended combinations:

Goal	File Trust	Publisher Trust
<b>High Critical Asset Protection</b> – For high protection for intellectual property and other confidential information	8	High
<b>Protection with Flexibility</b> – To protect your computers from risky files but allow automatic approval of more files with relatively low threat	6	Medium

When you enable both file and publisher reputation approvals, a file is approved if *either* its own reputation or its publisher’s reputation meets the thresholds you set.

You can adjust these settings to meet your own judgment on the tradeoffs, but setting the approval level at a very low trust level is not advisable. One way to see what the effect of approvals at different trust levels will be is to examine the File Catalog and the Publishers list in the console, grouped to show their contents by Trust.

To see files by trust category, choose **Assets > Files** on the console menu, click the **File Catalog** tab, and choose **Trust** on the *Group By* menu.

To see current publishers by trust category, choose **Rules > Software Rules** on the console menu, click the **Publishers** tab, and choose **Trust** on the *Group by* menu. This list includes only those publishers whose files have been inventoried on agent-managed computers or added by importing a certificate from a file on a computer without an agent.

## How File Reputation Approvals Work

File reputation approvals rely on the most specific information available for the files known to Bit9 SRS. A separate reputation approval rule (global or by policy) is created on the Bit9 Server for each file meeting the reputation threshold. The scope of a reputation approval is determined by the list of policies on which reputation is enabled. As with other file approvals, reputation approvals can behave like per-policy approvals or global approvals, depending on your reputation settings.

File reputation rules are not listed on the Bit9 Server, but you can view a list of files approved by reputation. See [“Views Related to Reputation Approvals”](#) on page 290.

Unlike other approvals, file reputation approvals are not pushed to endpoints automatically. There are three conditions that cause a reputation-based file approval to be sent to endpoints *on which reputation approval is enabled*:

- If the Bit9 Server has a record of a file being blocked *on any endpoint* and that file is later approved by reputation, the server begins sending the approvals of the file to agents immediately.
- If a user attempts to execute an instance of a reputation-approved file on a computer connected to the Bit9 Server, and if the server detects that the file satisfies the reputation trust threshold, the server will allow the agent to run the file immediately, and also will begin sending the approval to other agents.
- If the reputation-approved file is identified as an installer, the Bit9 Server begins sending the approval of the file to agents immediately.



Even if a file is approved by reputation and not blocked by another rule, until its approval is sent to agents because of one of the cases above, instances of the file may be locally unapproved and may block if the agent computer is disconnected from the server before the approval is distributed.

## Removal of Reputation Approval for a File

If the file reputation approval rule changes in a way that removes reputation approval from a file – by disabling reputation approval completely or by policy, by raising the approval threshold, or by lowering the file’s own reputation – the global approval for that file is eliminated from connected computers, and the file state in the File Catalog reverts to unapproved. If an instance of this file was executed during the time it was approved by reputation, that instance remains locally approved on the computer where it was executed.

Any explicit assignment of a ban or approval state to a file or its publisher takes precedence over a reputation approval.

### Note

Approval by file reputation involves a significant initial impact on the Bit9 Server as files are analyzed to see whether they would be approved according to Trust Level. In addition, disabling file approvals or changing the approval threshold has a similarly significant impact. Avoid unnecessary changes in file reputation rule configuration.

## How Publisher Reputation Approvals Work

When approval by publisher reputation is enabled, the list of all trusted publishers that meet the specified threshold is sent down to all computers. This allows Bit9 Agents that receive this publisher approval to approve new files from approved publishers as soon as they are seen for the first time, even if the computer is disconnected from the server when the new file arrives. In addition, the agent will approve all existing files from these publishers that were previously unapproved, unless they are explicitly banned.

Approval by publisher reputation has a low impact on the Bit9 Server and network traffic.

As with manual publisher approval, only files whose certificates meet all requirements described in [Approving or Banning by Publisher](#) can be approved by publisher reputation.

## Removal of Reputation Approval for a Publisher

Once a file is locally approved because of its publisher’s reputation, removal of *publisher* approval at a later time does not remove local approval of that file. Anything that removes approval from the publisher, including a change in reputation, a change in reputation approval settings, or completely disabling reputation approvals, affects only files that are encountered in the future.

If a publisher is no longer approved by reputation, its files can be returned to the unapproved state by manually removing the local approval on the Files on Computers or File Instance Details page for each instance. If a publisher is banned, however, that ban removes the approval from the file that was previously locally approved because of publisher reputation – it is not necessary to manually remove local approval for each instance.

Explicitly banning a file removes a local approval that occurred because of publisher approval.

## Reputation Approvals and Other Bit9 Rules

Reputation rules can be affected by other actions you perform on the console:

- Any explicit file rule that identifies a file by name or hash will automatically disable reputation control for that file. This includes global and policy-specific File Rules (bans and approvals), files on imported lists of hash approvals or bans, trusted directories, and manual publisher bans and approvals. Once a file is not controlled by reputation, it will no longer automatically get approved or unapproved based on reputation settings and thresholds.
- To allow reputation to control the state of a file with reputation disabled, you must remove the explicit rule (approval or ban) and then re-enable reputation for the file.
- Custom rules that directly block or allow access to a file will supersede reputation approvals by file or publisher.

## Creating Exceptions for Files and Publishers

In general, you should enable reputation approvals because you want to rely on the information in Bit9 SRS to eliminate a large number of unnecessary file blocks on trusted files. However, there might be a particular file or publisher that you do not want approved, regardless of its reputation in Bit9 SRS. You have the option of disabling reputation approvals for an individual file or publisher.

### Notes

If you create file or publisher exceptions *before* the reputation feature is enabled for the Bit9 Server, those files or publishers are unaffected by reputation rules. Exceptions added *after* reputation rules are enabled prevent reputation approval of newly discovered files and remove global approvals based on file reputation, but they do not undo local approval of files whose publisher was approved by reputation.

## Disabling Reputation Approvals for a File

You can disable reputation approvals for individual files. If you create the exception before enabling reputation rules on your server, it prevents any approvals by reputation for instances of the file. If you create the exception *after* enabling reputation rules, the reputation-approved file will revert to unapproved (both globally and locally) if no other approvals apply. If the file was already locally approved by some other means, however, (such as publisher approval or a custom rule), it will remain locally approved.

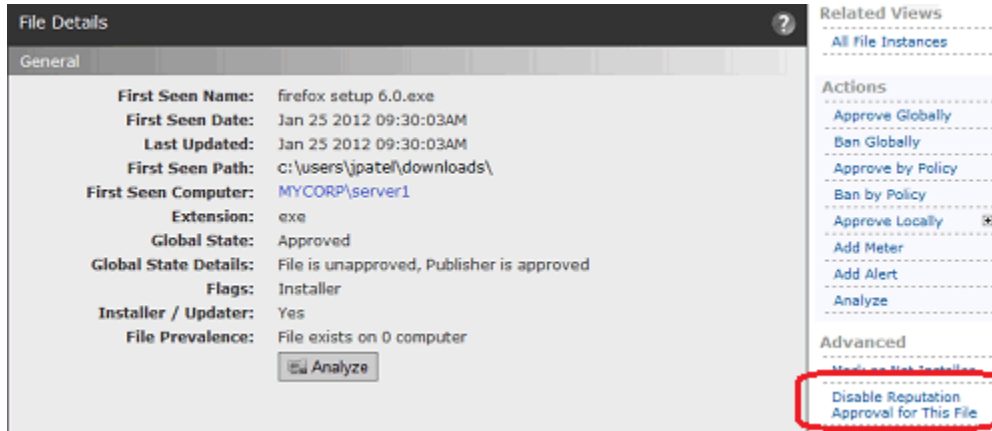
When you disable reputation for a file, it affects only that file, even if it is an installer.

### To disable reputation approval for a file:

1. Open the File Details or File Instance Details page for the file.
2. In the Advanced menu to the right of the main page, click on **Disable Reputation Approval for this File**. Reputation approvals are disabled for the file.

### To re-enable reputation approval for a file:

- Click the *Enable Reputation Approval for this File* option in the Advanced menu on the File Details or File Instance Details page.



## Disabling Reputation Approvals for a Publisher

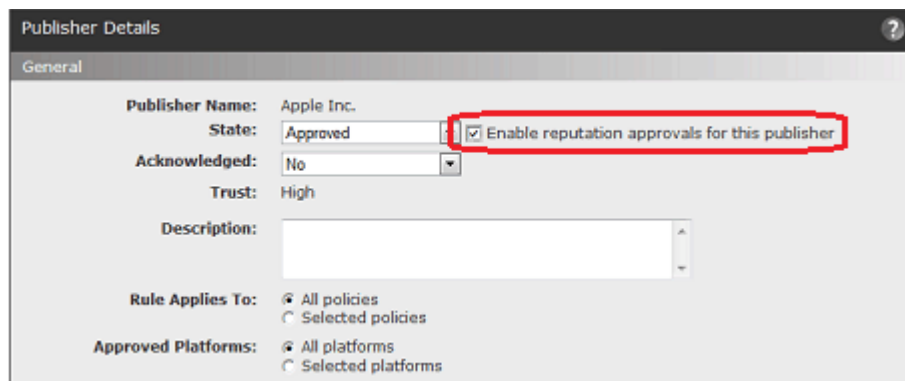
You can disable reputation approvals for individual publishers. If you create the exception before enabling reputation rules on your server, it prevents any approvals by reputation for instances of files from the publisher. If you create the exception after enabling reputation rules, however, any files from an approved publisher found on agent-managed computers prior to disabling the publisher will already be locally approved by reputation, and will not become unapproved if you disable the publisher. Only files first seen by this Bit9 Server *after* you disable approval for the publisher are unaffected by the publisher's reputation.

### To disable reputation approval for a publisher:

1. Open the Publisher Details page for the publisher.
2. Un-check the checkbox next to *Enable reputation approvals for this publisher*.
3. Click the **Save** button. Reputation approvals are disabled for this publisher.

### To re-enable reputation approval for a publisher:

- Check *Enable reputation approvals for this publisher* on the Publisher Details page.



## Enabling Reputation Approvals

This section describes enabling the reputation approvals feature for your Bit9 Server. Before enabling reputation approvals:

- Consider exceptions you want to create for files and publishers that you do not want approved by reputation. These exceptions should be created *before* you enable the feature. See [“Creating Exceptions for Files and Publishers”](#) on page 286 for details.
- Consider whether you would like reputation approvals to be available for all of your agent-managed computers or only those in certain policies. This choice is covered in the procedure below.

Keep in mind that although you can add file and publisher exceptions after you enable reputations for Bit9 Server, the publisher exceptions do not reverse any local approvals that have already occurred due to publisher reputation.

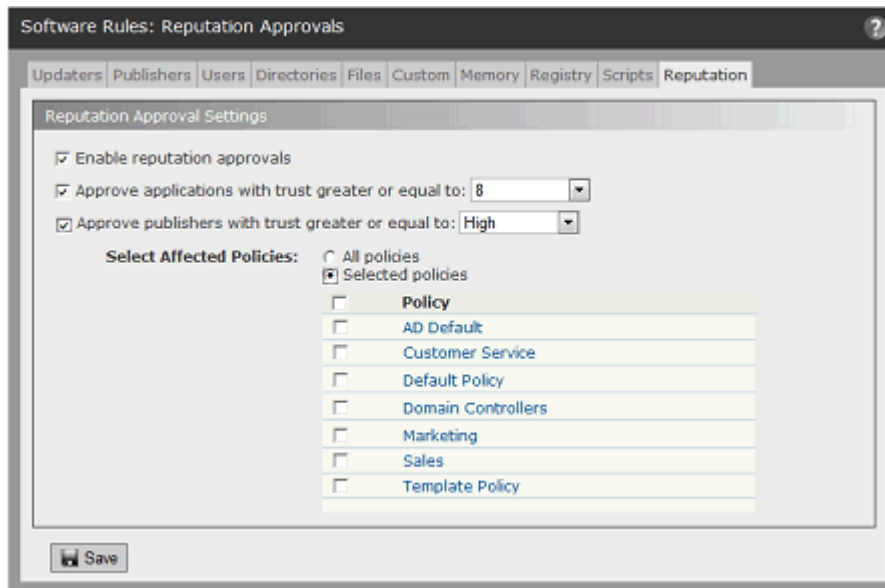
**To enable reputation approvals:**

1. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. On the Software Rules page, click the **Reputation** tab. The Reputation Approvals page appears.

**Note**

Bit9 SRS must be activated before you can enable Reputation Approvals. If no Reputation tab appears on the Software Rules page, Bit9 SRS is not activated. In this case, follow the instructions in [“Activating Bit9 SRS”](#) on page 643 before continuing with this procedure.

3. Click to check the box labeled *Enable reputation approvals*. This opens the fields on the page for editing.



4. To enable *file* approval by reputation, make sure the box next to *Approve applications with a trust greater or equal to* is checked and then choose a trust level from the menu. File trust choices range from 1 (very low trust) to 10 (highest trust). See [“Setting the Trust Level for Approvals”](#) on page 284 for recommendations.

5. To enable *publisher* approval by reputation, make sure the box next to *Approve publishers with trust greater or equal to* is checked and then choose a publisher trust level. Publisher trust has three values: *Low*, *Medium* and *High*.
6. Select the policies for which you want to enable reputation approvals:
  - a. To enable the rules for all policies, click the *All policies* radio button.
  - b. To enable the rules only for some policies, click the *Selected policies* radio button and check the box next to each policy you want to be affected by these rules.

**Note**

You also can enable or disable reputation approvals for a policy on its Edit Policy page.

7. When you have finished configuring reputation approvals, click the **Save** button at the bottom of the page and choose **OK** in the confirmation dialog. Reputation approvals are activated.

**Note**

Enabling file reputation approvals can require that very large numbers of file states are re-evaluated. You will not necessarily see changes in file state immediately in the console, but the server continues to process these changes in the background until all are up-to-date with the new approval rules. Full processing of the approvals may take several minutes.

## Modifying and Disabling Reputation Approvals

You can modify or disable the reputation approval features in the same place where they were enabled. Modifications include changing the file or publisher trust threshold and changing the policies affected by reputation approvals. If you choose, you also can disable one type of reputation approval (i.e., publisher or file) while leaving the other in place.

The effect of modifying or disabling reputation approvals depends upon what kind of approval you enabled. Changes in reputation approval also have different network impacts as rules are re-evaluated.

- Changing the approval threshold for file reputation approvals can have a very significant one-time impact on server and network traffic while the changes are processed. Evaluation and updating of the File Catalog will take a few minutes, but depending upon the number of agents and the size of the File Catalog, it could take from hours to days to send the new file state information to all agents.
- Disabling file approvals can have a very significant network impact and, as with changing the approval threshold, might require from hours to days before all agents are updated with the changes in file state.
- Changes in publisher approval rules or policy coverage do not have a significant impact.
- Disabling publisher approval does not undo any local file approvals that already occurred because of publisher reputation.

**To modify or disable the reputation approvals feature:**

1. On the **Rules > Software Rules** on the console menu and click the **Reputation** tab. The Reputation Approvals page appears,
2. Make any needed changes and click **Save**.

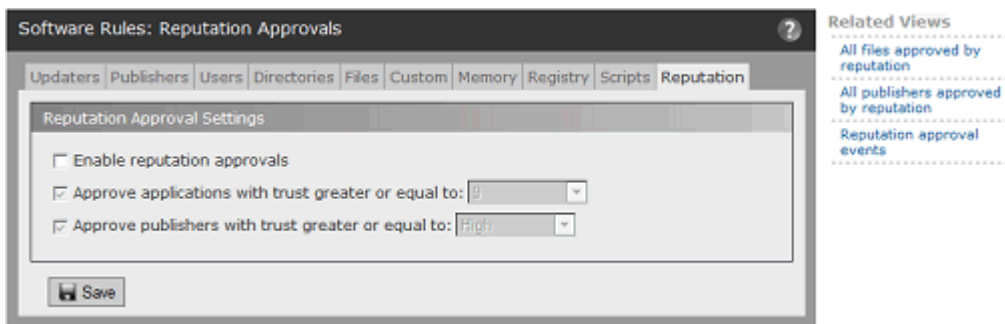
**Notes**

- You also can enable or disable reputation approvals for a policy on its Edit Policy page.
- You can create exceptions for files or publishers you don't want controlled by reputation approvals. See [“Creating Exceptions for Files and Publishers”](#) on page 286.

## Views Related to Reputation Approvals

The Related Views menu on the right side of the Reputation Approvals page provides links to additional information related to these approvals that is available in the console:

- **All files approved by reputation** – Clicking on this link shows the File Catalog page filtered to show all unique files globally approved by reputation.
- **All publishers approved by reputation** – Clicking on this link shows the Publishers tab of the Software Rules page filtered to show all publishers approved by reputation.
- **Reputation approval events** – Clicking on this link shows the Events page filtered to show all events related to reputation approvals (publisher and file).



These views can help you understand how reputation approvals are affecting your computers and perhaps point to changes you would like to make in the reputation approvals configuration, or in the state of specific files or publishers.

In other views that show files or publishers, you can see whether a file or publisher has been affected by reputation approvals by looking at these fields:

- **File State Reason** – If the file was approved by file reputation, this field shows *Reputation*. If the file has an approved publisher the File State can be *Approved by Reputation* even when File State Reason is something other than Reputation.
- **Publisher State Reason** – If the publisher for a file is approved by reputation, this field shows *Reputation*.

- **Reputation Enabled** (files) – The File Details and File Instance Details pages include a Reputation Enabled field that shows whether file reputation approvals are enabled for the current file. You can add this same field to the File Catalog and Files on Computers pages. Note that a value of *Yes* means that the file can be approved by reputation, not that it is approved.
- **Reputation Enabled** (publishers) – On the Publishers tab on the Software Rules page, you can add a column that shows whether reputation approvals are enabled for each listed publisher. As with files, a value of *Yes* means that the publisher can be approved by reputation, not that it is approved.





## Chapter 10

## Managing File-Signing Certificates

This chapter describes advanced features for using file-signing certificates in Bit9 file monitoring and enforcement activities. These features provide the following capabilities:

- **Certificate Discovery and Inventory** – Information about file-signing certificates discovered on agents and all certificates in their chains is collected and stored in the Bit9 Server database.
- **Enforcement by Certificate State** – Any certificate in a certificate chain may be approved or banned for a specific publisher, and its state can be used to approve or ban files managed by the Bit9 Platform.

### Platform Note

These certificate visibility and control features are available only for computers running Windows operating systems.

### Sections

Topic	Page
<a href="#">Overview</a>	<a href="#">294</a>
<a href="#">Summary of Certificate Management Features</a>	<a href="#">295</a>
<a href="#">Viewing Certificate Information</a>	<a href="#">295</a>
<a href="#">Viewing Certificates for a Publisher</a>	<a href="#">301</a>
<a href="#">Certificate Alerts</a>	<a href="#">303</a>
<a href="#">Certificate Events</a>	<a href="#">303</a>
<a href="#">Using Certificates for Enforcement</a>	<a href="#">304</a>

## Overview

The Bit9 Platform provides the ability to approve or ban a publisher by its *name*, as identified in a certificate. Files signed with certificates whose publisher name matches an approved publisher are approved unless banned by some other rule; files with certificates whose publisher name matches a banned publisher are banned. All files with a given publisher name in their certificate are affected by that publisher's state as defined on your Bit9 Server. These rules are described in “[Approving or Banning by Publisher](#)” on page 236.

The certificate management features described in this chapter add another layer of security and information to publisher approvals. While publisher names in certificates are not controlled by any central authority, certificates themselves are. A certificate identifies an individual, a server, a company, or other entity, and associates that identity with a public key. It provides generally recognized proof of identity based on public-key cryptography. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate; in this case, the entity is a file.

File-signing certificates are the final link in chains or paths of certificates. There is a root certificate, which identifies the entity that conferred the initial trust. That certificate might be used to sign an intermediary certificate, which then confers its trust to the final leaf certificate that specifically identifies the file. There can be more than one intermediary certificate in a path.

The Bit9 Agent reports all identifiable, valid certificates in the path of trust for signed files it discovers. Any certificate in the path of the signing certificate can be approved or banned. When a certificate is assigned a state of Approved or Banned (or left as Unapproved), that state applies only for a specific publisher of a leaf certificate. If the same certificate happens to appear in the certificate chain for a file signed by a different publisher, a separate certificate approval or ban is needed to affect that file.

### Note

In late 2013, Microsoft published security bulletin MS13-098 describing a flaw in the Authenticode signature verification that could allow remote code execution. In response, Microsoft announced availability of an update for all supported releases of Microsoft Windows to change how signatures are verified for binaries signed with the Windows Authenticode signature format.

If this change is enabled, Windows Authenticode signature verification will no longer allow extraneous information in the WIN\_CERTIFICATE structure, and Windows will no longer recognize non-compliant binaries as signed. Activation of this new behavior could cause files previously approved by publisher to block on Bit9-managed systems.

The change is included with Security Bulletin MS13-098, but (as of July 2014) will only be enabled on an opt-in basis. However, Microsoft states that it may make this a default behavior in a future release of Microsoft Windows.

See <https://technet.microsoft.com/library/security/2915720> for more information on this change.

## Summary of Certificate Management Features

Bit9 Certificate Management includes the following specific features:

- In the console menu, you choose **Assets > Certificates** to open the **Certificates table** page. The Certificates table shows all leaf certificates that have been used to validly sign or cosign files found on agent-managed computers, plus all certificates in the paths for those leaf certificates.
- Clicking on the View Details button next to a certificate in the table opens the **Certificate Details** page for that certificate. The Certificate Details page shows complete details for one certificate and has links to Related Views relevant to the certificate, such as a table of all files signed by the certificate.
- The **Publisher Details** page for each publisher includes an **All Certificates for This Publisher** panel. This panel shows all certificates that have this publisher name as the CN portion of the certificate Subject Name. It also shows the approval/ban state for each certificate in the certificate path for leaf certificates associated with that publisher, and allows you to add or remove approvals or bans for each certificate.
- Certificate-related fields are included on **File Details** and **File Instance Details** pages.
- On the **Advanced Options** tab of the **System Configuration** page, the **Certificate Options** panel includes settings that determine what requirements (such as key length and algorithm) a certificate must meet if it is to be used for approving files.
- Regardless of whether agent-based certificate revocation checks are enabled, the Bit9 Server validates certificates in its inventory on a recurring basis to make sure that they have not been revoked. This validation generally occurs on a weekly basis and involves downloading certificate revocation lists (CRLs) from registration authorities or making Online Certificate Status Protocol (OCSP) calls to OCSP responders. If you are monitoring network traffic, keep in mind that these downloads might involve a variety of sites in a variety of countries.  
Server-based validation checks are provided to inform administrators when the status a certificate changes, but they do not affect enforcement of rules. Enable agent-based revocation checks if you want revocations to affect rule behavior.
- Certificate-related **Events** and **Alerts** may appear when triggering conditions occur.

## Viewing Certificate Information

Certificate information is available in several locations in the Bit9 Console. This information can help you make decisions about whether to approve or ban certain certificates.

### Certificates Table

The Certificates table shows all leaf certificates that have been used to validly sign or cosign files found on agent-managed computers, plus all certificates in the paths for those leaf certificates. The table also provides access to the Certificate Details page for each

certificate – you can click either the View Details button or the Subject Name in the table to see details for a certificate.

**Note**

The Certificate table is a read-only page with no Action menu. Certificate state can be changed only in the context of a specific publisher, on the Publisher Details page. See “[Approving or Banning Certificates for a Publisher](#)” on page 306 for more information.

**To view the Certificates table:**

- On the console menu, choose **Assets > Certificates**.

Subject Name	Publisher ▲	Unique Signed Files
Adobe Systems Incorporated Digital ID Class 3 - Microsoft S...	Adobe Systems Incorporated	7
Certum CA Unizeto Sp. z o.o. PL	Certum CA	0
Certum Time-Stamping Authority Certum Certification Authori...	Certum Time-Stamping Authority	0
Class 3 Public Primary Certification Authority *VeriSign, I...	Class 3 Public Primary Certification Authority	0
Flexera Software LLC Digital ID Class 3 - Microsoft Softwar...	Flexera Software LLC	2
GeoTrust Global CA GeoTrust Inc. US	GeoTrust Global CA	0
GlobalSign ObjectSign CA ObjectSign CA GlobalSign nv-sa B...	GlobalSign ObjectSign CA	0
GlobalSign Primary Object Publishing CA Primary Object Publ...	GlobalSign Primary Object Publishing CA	0
GlobalSign Root CA Root CA GlobalSign nv-sa BE	GlobalSign Root CA	0
BE GlobalSign nv-sa RootSign Partners CA GlobalSign RootS...	GlobalSign RootSign Partners CA	0
timestampinfo@globalsign.com GlobalSign Time Stamping Autho...	GlobalSign Time Stamping Authority	0
Google Inc Digital ID Class 3 - Netscape Object Signing Go...	Google Inc	1
Google Inc Digital ID Class 3 - Java Object Signing Google...	Google Inc	353
Google Inc Digital ID Class 3 - Netscape Object Signing Go...	Google Inc	1
Google Inc Digital ID Class 3 - Netscape Object Signing Go...	Google Inc	66
Microsoft Code Signing PCA Copyright (c) 2000 Microsoft Cor...	Microsoft Code Signing PCA	0

The default table includes selected columns with key information about each certificate. As with any Bit9 table, you also may add or remove columns from the table view using the *Show/Hide Columns* panel (See “[Bit9 Console Tables](#)” on page 58 for more information about customizing a table view.). [Table 40](#) shows the possible fields available on the Certificates table and also the Certificate Details page. Keep in mind that some of these fields are not shown by default in the table.

**Table 40:** Fields in Certificates Table and Details Pages

Field/Column	Source	Appears	Description
<b>Note:</b> In the Where column, T = Table page, D = Details page			
Subject Name	Cert	T, D	Distinguished name of the subject of the certificate, in this case the signer of the file. In the table, the name is shortened, but a tooltip provides a full length Subject Name. Clicking on the name in the table opens the details page for this certificate.
Publisher	Cert	T, D	Publisher name as identified by the CN portion of the Subject Name in the certificate. If this publisher signed any files in the File Catalog, clicking the name opens the Publisher Details page. Some of the "Publishers" listed are certificate authorities, not actual software publishers, and so do not have linked names.
Unique Signed Files	Bit9	T, D	Number of unique files in the File Catalog signed by this certificate. If greater than zero, clicking on the number opens the File Catalog filtered to show these files.
Path Position	Cert	T	Position of this certificate in the certificate path cataloged on the server. The possible values are: Root, Intermediary, Leaf. See " <a href="#">Path Position and Agent Differences</a> " on page 306 for details about certificate path position, variations among agents, and the impact on certificate management.
Root Certificate	Cert	D	Is this a root certificate? The possible values are: Yes, No.
Global State	Bit9	T,D	Effective state of this certificate derived from the following: Publisher State of the publisher identified in this certificate; Certificate State; Certificate Path State, and certificate configuration settings. See " <a href="#">Certificate Global State</a> " on page 308 for global certificate state determination, values, and how it interacts with the states of other objects.
Certificate State	Bit9	T	State assigned to the certificate for this publisher. The possible values are: Approved, Unapproved, Banned. See " <a href="#">Certificate Global State</a> " on page 308 for a description of how this affects global certificate state and file state.
Certificate State Details (in details) Global State Details (in table)	Bit9 & Cert	T,D	Detailed description of all of the factors contributing to Certificate Global State. See " <a href="#">Certificate Global State</a> " on page 308 for more information.

Field/Column	Source	Appears	Description
Valid From	Cert	T,D	Date this Certificate is valid from. Format is MMM DD YYYY HH:MM:SS AM/PM (UTC).
Valid To	Cert	T,D	Date this Certificate is valid to. Format is MMM DD YYYY HH:MM:SS AM/PM (UTC).
Signature Algorithm	Cert	T,D	Algorithm used to create the certificate's signature. Typical values: MD2RSA, MD5RSA, SHA1RSA, SHA256RSA. See " <a href="#">Certificate Approval Configuration Choices</a> " on page 304 for configuration settings related to this field.
Thumbprint	Cert	T,D	SHA1 hash value of this certificate.
Certificate ID	Bit9	T,D	Unique Bit9-generated hash identifier for this certificate.
First Seen Date	Bit9	T,D	Date and time this certificate was first seen and inventoried on this Bit9 server.
Last Modified Date (in details) Date Modified (in table)	Bit9	T,D	Date and time the record for this certificate was last modified on this Bit9 Server.
Description	Bit9	T,D	An editable field in which console users can add or modify a comment about this certificate.
Last Validation Date	Bit9	T,D	Last date and time when this certificate was validated on the Bit9 Server. Certificates are validated when discovered and periodically re-checked.
Public Key Algorithm	Cert	T,D	Algorithm used to produce the public key.
Public Key Size	Cert	T,D	Size of the public key for this certificate. See " <a href="#">Certificate Approval Configuration Choices</a> " on page 304 for size settings.
Serial Number	Cert	T,D	A field in the certificate containing a number that is unique among certificates from its issuing certificate authority.
Type	Cert	T,D	Indicates whether a certificate was embedded or detached or both, and whether the signature was used to sign the file or to countersign the signature, usually for timestamp validation. Leaf certificates only. The possible values are: Embedded, Detached, Signer, Cosigner. Each certificate has two or more of these values. See " <a href="#">Certificate Types</a> " on page 305 for details about type and its impact on certificate management.

Field/Column	Source	Appears	Description
Validation Error (in Table) Validation Message (in Details)	Cert	T,D	Shows any error messages returned when the certificate is checked. If the certificate check produces no errors, this field will be blank. See <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/aa377590(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/aa377590(v=vs.85).aspx</a> for a list of possible messages.  Many certificates show validation errors for reasons that are not necessarily an indication of significant risk. For example, a certificate authority may stop providing information (and thus validation) for older certificates.
History	Bit9	D	Panel includes the following where appropriate: <ul style="list-style-type: none"> <li>• First Seen Date – The date and time this certificate was first seen in your Bit9 environment.</li> <li>• Last Modified by – The console user that made the most recent change to certificate state (not in table).</li> <li>• Last Modified Date – The date and time when the most recent change to certificate state was made.</li> </ul>
Certificate Path	Cert	D	Panel shows this certificate in the context of its path. Each item in the list (except for the current certificate) is a link to the certificate details for other certificates in the path.

## Searching, Sorting and Grouping on the Certificates Table

You can use any of the standard table customization methods to show or find specific certificates. For example, you can use the Show/Hide Filters menu to search for a particular certificate by Subject Name or Hash, or use the *Group by* menu to organize the Certificates by certain fields. The *Group by* menu includes the following choices:

- Subject Name
- Publisher
- Unique Signed Files
- Path Position
- Global State
- Certificate State
- Valid From
- Valid To
- Signature Algorithm
- Thumbprint

## Certificate Details

The Certificate Details page shows complete details for one certificate. It also has links to Related Views relevant to the certificate. [Table 40](#) describes the fields that appear on this page.

### To view the Certificates Details page for one certificate:

- In the Certificates table or the certificates section of a Publisher Details page, click on the View Details button or the Subject Name for the certificate.

In other locations in which certificates information is displayed, such as the Events table, you can click on the Subject Name of a certificate to see its details.

**Certificate Details**

**General**

**Publisher:** [Microsoft Corporation](#)  
**Subject Name:** Microsoft Corporation AOC Microsoft Corporation Redmond Washington US  
**Thumbprint:** 6041c8f759c9c9a2970bb8af43c6ae17368d0d32  
**Last Validation Date:** Jan 22 2013 01:31:29 AM  
**Unque Signed Files:** [67](#)  
**Description:**

**Certificate State For Publishers**

Publisher	Certificate Global State	Certificate State Details
<a href="#">Microsoft Corporation</a>	Unapproved	Certificate is Unapproved, Publisher is Unapproved, Certificate Path is Unapproved

**Certificate Properties**

**Serial Number:** 330000008701c97bf14c00b9de000100000087  
**Signature Algorithm:** sha1RSA  
**Valid From:** Jul 26 2012 04:50:38PM  
**Valid To:** Oct 26 2013 04:50:38PM  
**Root Certificate:** No  
**Type:** Embedded Signer  
**Public Key Algorithm:** RSA  
**Public Key Size:** 2048

**History**

**First Seen Date:** Jan 22 2013 01:31:24 AM  
**Last Modified By:** System  
**Last Modified Date:** Jan 22 2013 01:31:24 AM

**Certificate Path**

**Subject Name**

- [Microsoft Root Certificate Authority microsoft.com](#)
- [Microsoft Code Signing PCA Microsoft Corporation Redmond Washington US](#)
- [Microsoft Corporation AOC Microsoft Corporation Redmond Washington US](#)

**Related Views**

- [All files signed by this certificate](#)
- [All unique files signed by this certificate](#)
- [Files signed by certificates with this certificate in path](#)
- [All child certificates for this certificate](#)
- [All events for this certificate](#)

In the Certificate Details, if the Publisher name is highlighted as a link, you can click on it to go to the details page for the publisher of this certificate. You also can click on any highlighted certificate name in the Certificate Path panel to view its details. If this certificate has signed files, clicking on the number next to the Unique Signed Files field displays a File Catalog view filtered to show those files. Note that for *intermediate* and *root* certificates, the Publisher names for intermediate and root certificates are *not* links.



## Related Views Menu on Certificate Details

The Certificate Details menu includes a Related Views menu that can provide additional information about a certificate and how it is being used in your environment. Not all Related Views choices are available for all certificates. The view options are:

- **All files signed by this certificate** – Displays the Find Files page filtered to show all file instances signed by this certificate (i.e., for which this is the “leaf” certificate).
- **All unique files signed by this certificate** – Displays the File Catalog page filtered to show all unique files signed by this certificate.
- **Files signed by certificates with this certificate in path** – Displays the Find Files page filtered to show all file instances that have this certificate in their certificate path.
- **All child certificates for this certificate** – Displays the Certificates page filtered to show child certificates at any level below this certificate.
- **All events for this certificate** – Displays the Events page filtered to show events related to this certificate. This includes creation or deletion of bans and approvals, discovery or addition of certificates, and certificate checks.

## Viewing Certificates for a Publisher

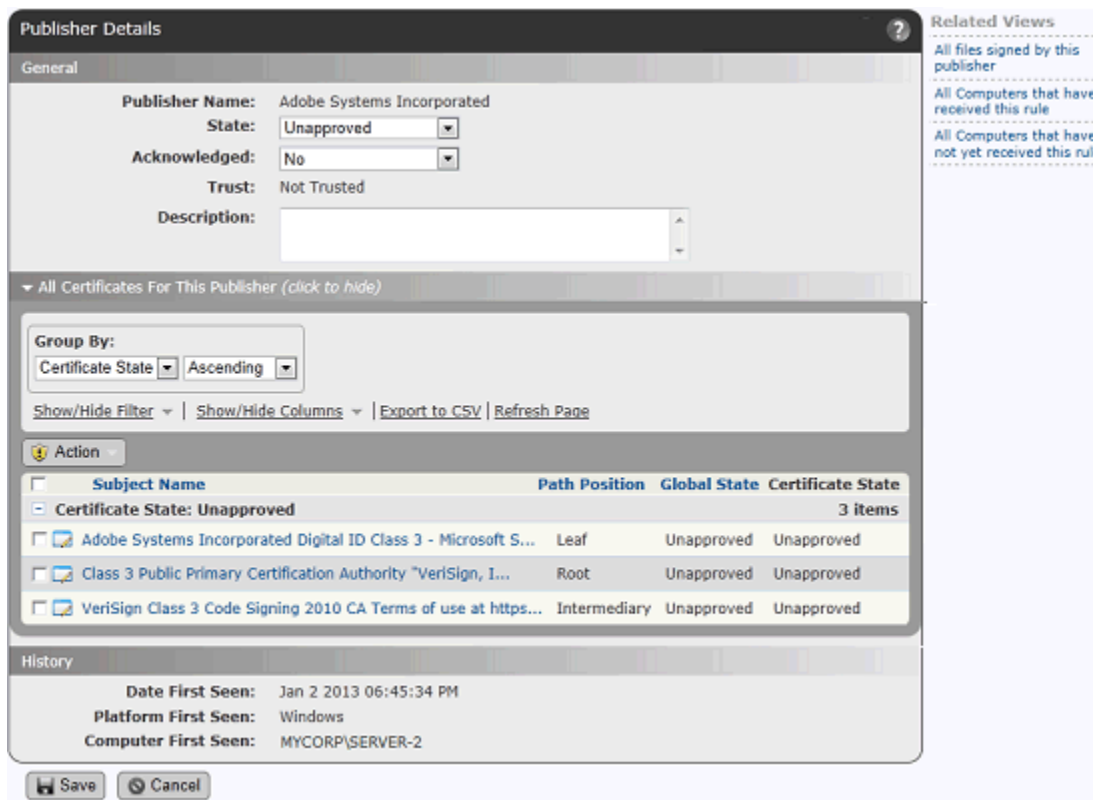
The Publisher Details page includes a panel entitled *All Certificates for This Publisher*. Because this panel has the potential to be long, it can be collapsed and expanded on the page by clicking the panel name.

### To view certificates in the Publisher Details page:

1. Click on the highlighted name of a publisher.

**Note:** The publisher name appears in many places, including events, file details, and certificate details. If it is not highlighted, it is not a software publisher that signs files directly but may be a certificate authority that signs certificates that sign files.

2. If the certificates for the publisher are not shown, click on **All Certificates for this Publisher**.



The panel shows all leaf certificates for this publisher, and all root and intermediate certificates associated with these leaf certificates. It is similar to the Certificates table, and you can modify it using standard filter, column, and grouping tools for tables. For any certificate shown, you can go to its details page by clicking on the View Details button or Subject Name.

The table of certificates on the Publisher Details page has an Action menu. Using this menu, you can ban, approve, or remove an approval or ban from a certificate in the context of the current publisher. This is described in more detail in [“Approving or Banning Certificates for a Publisher”](#) on page 306.

## Certificate Fields in File/File Instance Details

There are certificate-related fields in the File Catalog, Files on Computers, File Details, and File Instance Details pages in the console. In most cases, the certificate name or hash provides a link from the file information to full information about the certificate that has signed the file. Certificate information is also included in the Global State Details in on all of these pages. See [Chapter 7, “File and Publisher Information,”](#) for more information.

[Table 41](#) shows where certificate-related fields appear on file pages.

**Table 41:** Certificate-Related Fields in File Table and Details Pages

Field	File Catalog	Files on Computers	File Details	File Instance Details
Certificate			Link	X

Field	File Catalog	Files on Computers	File Details	File Instance Details
Certificate Type			X	X
Certificate Global State	X	X	X	X
Certificate Hash	Link			
Certificate State Reason	X	X		
Certificate Subject Name	X	X		
Detached Certificate Subject Name (Detached Certificate in Details pages)		X		Link
Detached Certificate Type				X
Detached Certificate State				X

## Certificate Alerts

There are two certificate-related alerts that may be of particular interest if you are using certificates as part of your security enforcement plan:

- **New Certificate Alert** – Alerts subscribers when a file with a certificate for a publisher not yet listed in the Bit9 Console is discovered, and when a new certificate is imported directly into the Bit9 Server. By default, this alert is triggered when a new certificate for any publisher is detected. However, it can be configured to trigger only for new certificates for specific publishers.
- **Revoked Certificate Alert** – Alerts subscribers when a certificate known to this Bit9 Server is revoked. By default, this alert is triggered when a certificate for any publisher is revoked. However, it can be configured to trigger only for specific publishers.

There is a special mail template for informing users about certificate discovery or revocation.

See [“Using Bit9 Alerts”](#) on page 494 for more information about configuring, enabling, and responding to alerts.

## Certificate Events

Bit9 reports events associated with file-signing certificates. These events appear on the Events page in the console and are also available in Syslog output. The event description for certificate-related events includes the Subject Name. On the console Events page, Subject Name is a link to the Certificate Details page.

See the separate *Bit9 Event Integration Guide* to for more on event subtypes (the unique Bit9 identifier for an event) for certificates. The subtypes fall into two types:

- **Discovery events** – These are events that have to do with the certificates themselves, independent of their Bit9 state.
- **Policy Enforcement events** – These are events that report addition or removal of a Bit9 ban or approval for a certificate.

See “[Event Reports](#)” on page 482 for more information about viewing events in the Bit9 Console. See the separate document.

## Certificates in External Views

Bit9 provides public views into the database of files and events as an alternative to the console. You can create your own reporting and data analysis solutions through the use of these public views. The certificate-related event subtypes described in the previous section may be included in the ExEvents view. In addition, certificate metadata is included with file information in the following views:

- **ExFileCatalog** – Metadata for all unique hashes
- **ExFileInstances** – Metadata of all file instances on all computers
- **ExDeletedFileInstances** – Metadata of all deleted file instances

See [Appendix A, “Live Inventory SDK: Database Views,”](#) for more information about accessing the external views of the Bit9 database.

## Using Certificates for Enforcement

The previous sections of this chapter focused on information Bit9 provides about certificates. This section describes certificate approvals and bans, and their effect on file state. The following is a summary of the certificate approval and ban features:

- **Certificate Approval Settings** – The System Configuration page has Advanced Options that affect whether certain certificates can be globally approved.
- **Manageable Certificate Types** – Regardless of configuration choices, not all discovered certificates can be approved or banned.
- **Path Position and Agent Differences** – For the same certificate/publisher combination, different agents can have different certificate paths, and the path on the server may match some or none of those currently on the agents.
- **Certificate State** – Approving or banning a certificate (or removing approvals and bans) determines Certificate State for a specific certificate for a specific publisher.
- **Certificate Global State** – Other factors interact with Certificate State to determine the Certificate Global State, which is its effective state.
- **Impact on File State** – Certificate Global State interacts with other rules and states to determine the state of a file signed by a particular certificate or one of its children.
- **Certificate Ban Setting** – Each computer’s Policy has an Advanced Setting that determines whether certificate bans are effective.

A key point to keep in mind when preparing to approve or ban certificates is that you must specify the state *in each publisher for which you want it to be effective*.

## Certificate Approval Configuration Choices

To be effective for approving a file, all certificates in the certificate chain for that file must be considered valid by Windows. For example, current root certificates must be installed for a certificate to be accepted.

In addition, there are configuration settings on the Advanced tab of the System Configuration page that determine whether a certificate approval is effective in determining the state of a file signed by that certificate. “[Determining Which Certificates Can Approve Files](#)” on page 242 describes these configuration options in detail.

Remember that certificates can be approved and banned themselves, and also can be used to approve or ban a publisher by name. Keep the following in mind when setting or viewing Certificate Options on the Advanced Options page:

- You can approve a certificate that does not meet these configuration requirements, and the certificate itself will show a Certificate State of Approved. However, the Certificate Global State (the effective state) of such a certificate cannot be Approved.
- Certificate Options choices have no effect on cosigner certificates.
- Certificate Options choices do not prevent any certificate from being banned, or prevent the value of Certificate Global State from being Banned. See “[Certificate Global State](#)” on page 308 for more information.
- The Expired Certificates option on the System Configuration/Advanced Options tab does not affect the ability to globally approve a *certificate*; it determines whether an expired certificate can be used to approve a file by *publisher*. If the box is checked, then if a file has a certificate that has expired but was used to sign the file during the valid period, the certificate may be used for approval by publisher. If not checked, expired certificates may not be used to approve files by publisher. This setting does not affect Certificate Global State.

## Certificate Types

The Certificate Details page includes a Certificate Type field, which has a value for leaf certificates only. Certificate type indicates what the leaf certificate is being used for and how it is associated with a file. Type is some combination of the following terms:

- **Embedded** – The digital signature for a file is embedded in a non-executable part of the file itself.
- **Detached** – The file to be signed is hashed into a digest and the digital signature is applied to the digest and included in a separate catalog file, which can contain certificates for multiple files.
- **Signer** – The certificate is the code-signing certificate for files it signs.
- **Cosigner** – The certificate is a cosigner (also called “countersigner”) certificate for files it signs. Cosigner certificates are normally used for time stamping.

Each instance of a leaf certificate must be either embedded or detached, and it must be a signer or a cosigner, so the minimum number of descriptors in the Type field for any certificate is two. There could be more than two since the same certificate can be used in different ways and so can have different types. One certificate in the Certificates Table may display its Type as Embedded Detached Signer, for example, or some other combination of these terms.

### Important

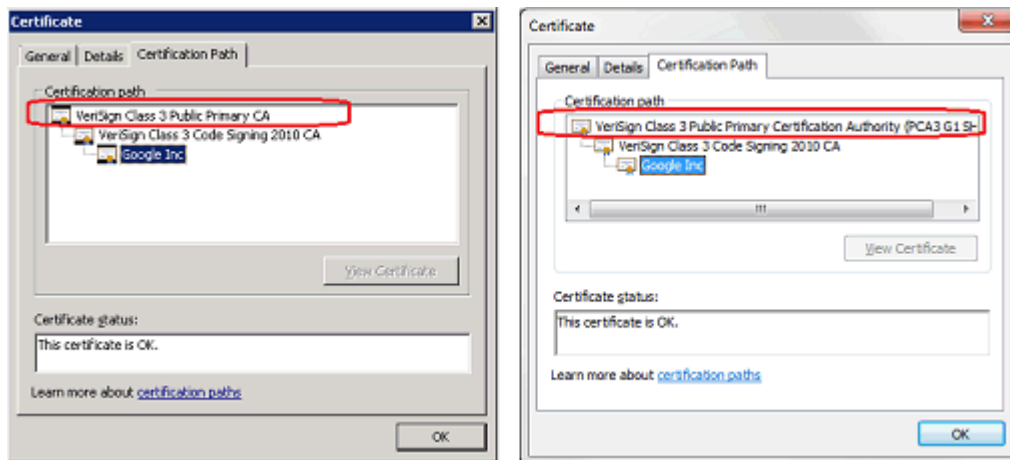
Only certificates identified and used as the Signer for a file may be approved or banned. Cosigner certificates are not assigned a state by Bit9.

## Path Position and Agent Differences

When you view the Publisher Details page, the *All Certificates for This Publisher* panel shows all certificates in the path. You can approve or ban any of these certificates. Before doing that, however, consider the different impact of approving or banning at different points on the path.

Certificate paths for the same leaf certificate may vary on different agents, or between an agent and the server. This could occur when the same file is received from different sources, or when one computer has updaters enabled and another does not. Agents update their certificate paths over time to minimize these differences.

Because of the potential for path differences, approving or banning intermediary or root certificates might not have the results you expect. The following example shows the same leaf certificate (same Issuer and Serial Number) with different root certificates:



If you approved one of these roots and expected that to take care of all instances of the leaf, you would not see the desired results on all agents. Path differences might be less of an issue for internally signed certificates for which you control the entire certificate path.

To reduce certificate path variation, keep your certificate stores on agents and the server current. Also, make sure that operating system updaters and other key application updaters are allowed to run so that you have the latest versions of signed files.

## Approving or Banning Certificates for a Publisher

You approve or ban a certificate in the context of a publisher. The certificate state is effective only within that publisher; if a certificate is used by multiple publishers, you must assign its state in each.

Approving or banning a certificate defines its Certificate State, which can be Approved, Banned, or Unapproved. The effective certificate state, called Certificate Global State, is what is applied to files signed by that certificate. A certificate's Global State depends on the following: the Certificate State, the state of other certificates in its path, the Publisher State, and (for approvals) certificate configuration choices. See [“Certificate Global State”](#) on page 308 to see how different Certificate Global States are produced.

**To approve or ban a certificate:**

1. Make sure you have set the appropriate Certificate Options on the System Administration Advanced Options tab. These determine which certificates may be used for approvals. See “[Determining Which Certificates Can Approve Files](#)” on page 242.
2. Locate the certificate(s) you want to approve or ban, and then open the Publisher Details page for the publisher to which you want this approval or ban applied.

**Note:** You may locate a certificate first and click on its publisher name (e.g., from the File Details page, the Events page, or the Certificates table); or if you know the publisher for the certificate, open its details page directly.

3. If the certificates for the publisher are not already showing, click on **All Certificates for this Publisher**.

**Publisher Details**

General

**Publisher Name:** Adobe Systems Incorporated  
**State:** Unapproved  
**Acknowledged:** No  
**Trust:** Not Trusted  
**Description:**

▼ All Certificates For This Publisher (click to hide)

**Group By:**  
Certificate State | Ascending

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

**Action**

<input type="checkbox"/>	Subject Name	Path Position	Global State	Certificate State
<input type="checkbox"/>	<b>Certificate State: Unapproved</b> 3 items			
<input type="checkbox"/>	Adobe Systems Incorporated Digital ID Class 3 - Microsoft S...	Leaf	Unapproved	Unapproved
<input type="checkbox"/>	Class 3 Public Primary Certification Authority "VeriSign, I...	Root	Unapproved	Unapproved
<input type="checkbox"/>	VeriSign Class 3 Code Signing 2010 CA Terms of use at https...	Intermediary	Unapproved	Unapproved

**History**

**Date First Seen:** Jan 2 2013 06:45:34 PM  
**Platform First Seen:** Windows  
**Computer First Seen:** MYCORP\SERVER-2

Save Cancel

4. In the *All Certificates for this Publisher* panel, check the boxes next to any certificates you want to approve or ban. Note that all of the checked certificates must have the same state applied to them – that is, you cannot simultaneously approve some certificates and ban others.
5. On the Action menu, choose **Approve Certificates** or **Ban Certificates**. The Certificate State of the checked certificates is changed to the state you selected.

See “[Certificate Global State](#)” on page 308 to see how a Certificate State of Approved, Unapproved, or Banned interacts with other states and rules to produce Certificate Global State.

**To remove a certificate approval or ban:**

1. On the Publisher Details page, check the certificates whose state you want to change. Note that you can select a combination of banned and approved certificates for this operation.
2. On the Action menu, choose **Remove Approval or Ban**. The Certificate State of all checked certificates becomes Unapproved.

**Certificate Global State**

The Certificate Global State is the effective state of a certificate. The possible values for Certificate Global State:

- Unapproved
- Approved
- Banned
- Approved By Policy
- Banned By Policy
- Mixed

Certificate Global State is determined by the following factors:

- **Certificate State** – Values are Unapproved, Approved, or Banned.
- **Publisher State** – Values are Unapproved, Approved, Banned, Approved By Policy, or Banned By Policy.
- **Certificate Path State** – Values are Unapproved, Approved, Banned, or Mixed (some certificates in the chain are Approved and some are Banned).
- **Certificate Key Length and Algorithm** – Does this certificate meet System Configuration/Advanced Settings requirements.

For any certificate, you can view the factors that contribute to Certificate Global State on the Certificates (table) page or the Certificate Details page. The *Certificate State for Publishers* panel on the details page summarizes the relevant factors.

The screenshot shows a 'Certificate Details' window with a 'General' tab. Below the general information, there is a section titled 'Certificate State For Publishers' which contains a table. The table has three columns: 'Publisher', 'Certificate Global State', and 'Certificate State Details'. The data row shows 'XYZ Software Inc.' with a 'Certificate Global State' of 'Unapproved' and 'Certificate State Details' of 'Certificate is Approved: Public Key Size less than Minimum Key Size (4096), Publisher is Approved, Certificate Path is Unapproved'.

Publisher	Certificate Global State	Certificate State Details
XYZ Software Inc.	Unapproved	Certificate is Approved: Public Key Size less than Minimum Key Size (4096), Publisher is Approved, Certificate Path is Unapproved



In the example above, the Certificate Global State is Unapproved. In the Certificate State Details, you can see that although the state of the certificate itself is Approved, its public key size is less than the minimum specified on the System Configuration/Advanced Options page, which is what prevents its global state from being Approved. Note that if a certificate fails to meet more than one configuration requirement (e.g., both the minimum key size and the allowed algorithm specifications), only one of the two reasons appears in Certificate State Details.

The following examples may help clarify the way these values interact with each other to produce Certificate Global State. All possible combinations are shown in [Table 42](#), “Determining Certificate Global State”, on page 311.

### Example 1: All States and Configuration Allow Approval

Condition	Example/Comments
If the certificate meets the minimum key size configuration...	Minimum Certificate Key Size: 1024 Key length of this certificate: 2048
...and its algorithm type is not configured to be ignored...	Certificate Signature Algorithms to Ignore: Only MD2RSA is checked Signature Algorithm of this certificate: SHA1RSA
...and the certificate has a countersignature if required...	.
...and the certificate has not been found to be revoked in the configured revocation checks...	
...and the leaf Certificate State is Approved...	A console user chose to approve the certificate.
...and the Publisher State is Approved...	The publisher was approved by a console user or by reputation.
...and no other certificate in this certificate's path is Banned...	The state of the Certificate Path is shown in the Certificate Details
<b>...then the Certificate Global State is Approved.</b>	This is the state that will affect files signed by the certificate.

**Example 2: Certificate Does Not Meet a Configuration Requirement**

Condition	Example/Comments
If the certificate meets the minimum key size configuration...	Minimum Certificate Key Size: 1024 Key length of this certificate: 2048
but its algorithm type is configured to be ignored...	Certificate Signature Algorithms to Ignore: Has MD2RSA and SHA1RSA checked Signature Algorithm of this certificate: SHA1RSA
...and the Certificate State is Approved...	
...and the Publisher State is Approved...	
...and no other certificate in this certificate's path is Banned...	
<b>...then the Certificate Global State is Unapproved.</b>	Although all other criteria for approval were met, the certificate algorithm is not allowed for approvals.

**Example 3: Banned Certificate in the Path**

Condition	Example/Comments
Whether or not the certificate meets the minimum key size...	
...and no matter whether it meets any of the other Advanced Options requirements...	
...and if the Publisher State is Approved or Unapproved and does not have any policy restrictions...	
...if this certificate or any certificate in it the certificate path is Banned...	
<b>...then the Certificate Global State is Banned.</b>	Although Certificate Global State is Banned, the ban's effectiveness on each agent depends upon <i>Block files with banned publishers or certificates</i> on the Advanced Settings of the agent's policy. This setting is active by default.

**Example 4: Mixed Global State**

Condition	Example/Comments
If the Publisher State is Approved by Policy...	
...and if this certificate or any certificate in it the certificate path is Banned...	
<b>...then the Certificate Global State is Mixed.</b>	Certificate Global State acts as Unapproved for policies with publisher approval. Certificate Global State acts as Banned for policies not included in the publisher approval if banning by certificates is allowed in the policy.

Table 42 shows how different combinations of Certificate, Publisher, and Certificate Path states produce different Certificate Global states. All of these outcomes assume that all certificates in the path meet the configuration requirements specified on the System Configuration Advanced Options page. Where “(by Policy)” appears in parentheses in the table, the Certificate State shown is not *specified* as being by policy but is *effectively* “by Policy” because Publisher State is Approve by Policy or Ban by Policy.

**Table 42:** Determining Certificate Global State

#	Certificate State	Publisher State	Certificate Path State	Certificate Global State
1	Unapproved	Unapproved	Unapproved	Unapproved
2	Approved	Unapproved	Unapproved	Approved
3	Banned	Unapproved	Unapproved	Banned
4	Unapproved	Approved	Unapproved	Approved
5	Approved	Approved	Unapproved	Approved
6	Banned	Approved	Unapproved	Banned
7	Unapproved	Banned	Unapproved	Banned
8	Approved	Banned	Unapproved	Banned
9	Banned	Banned	Unapproved	Banned
10	Unapproved	Approved By Policy	Unapproved	Approved By Policy
11	Approved (by Policy)	Approved By Policy	Unapproved	Approved By Policy
12	Banned (by Policy)	Approved By Policy	Unapproved	Mixed
13	Unapproved	Banned By Policy	Unapproved	Banned By Policy
14	Approved (by Policy)	Banned By Policy	Unapproved	Mixed
15	Banned (by Policy)	Banned By Policy	Unapproved	Banned By Policy
16	Unapproved	Unapproved	Approved	Approved
17	Approved	Unapproved	Approved	Approved
18	Banned	Unapproved	Approved	Banned
19	Unapproved	Approved	Approved	Approved
20	Approved	Approved	Approved	Approved
21	Banned	Approved	Approved	Banned
22	Unapproved	Banned	Approved	Banned
23	Approved	Banned	Approved	Banned
24	Banned	Banned	Approved	Banned
25	Unapproved	Approved By Policy	Approved (by Policy)	Approved By Policy
26	Approved	Approved By Policy	Approved (by Policy)	Approved By Policy
27	Banned (by Policy)	Approved By Policy	Approved (by Policy)	Mixed

#	Certificate State	Publisher State	Certificate Path State	Certificate Global State
28	Unapproved	Banned By Policy	Approved (by Policy)	Mixed
29	Approved (by Policy)	Banned By Policy	Approved (by Policy)	Mixed
30	Banned (by Policy)	Banned By Policy	Approved (by Policy)	Mixed
31	Unapproved	Unapproved	Banned	Banned
32	Approved	Unapproved	Banned	Banned
33	Banned	Unapproved	Banned	Banned
34	Unapproved	Approved	Banned	Banned
35	Approved	Approved	Banned	Banned
36	Banned	Approved	Banned	Banned
37	Unapproved	Banned	Banned	Banned
38	Approved	Banned	Banned	Banned
39	Banned	Banned	Banned	Banned
40	Unapproved	Approved By Policy	Banned (by Policy)	Mixed
41	Approved (by Policy)	Approved By Policy	Banned (by Policy)	Mixed
42	Banned (by Policy)	Approved By Policy	Banned (by Policy)	Mixed
43	Unapproved	Banned By Policy	Banned (by Policy)	Banned By Policy
44	Approved (by Policy)	Banned By Policy	Banned (by Policy)	Mixed
45	Banned (by Policy)	Banned By Policy	Banned (by Policy)	Banned By Policy
46	Unapproved	Unapproved	Mixed*	Banned
47	Approved	Unapproved	Mixed*	Banned
48	Banned	Unapproved	Mixed*	Banned
49	Unapproved	Approved	Mixed*	Banned
50	Approved	Approved	Mixed*	Banned
51	Banned	Approved	Mixed*	Banned
52	Unapproved	Banned	Mixed*	Banned
53	Approved	Banned	Mixed*	Banned
54	Banned	Banned	Mixed*	Banned
55	Unapproved	Approved By Policy	Mixed* (by Policy)	Mixed
56	Approved (by Policy)	Approved By Policy	Mixed* (by Policy)	Mixed
57	Banned (by Policy)	Approved By Policy	Mixed* (by Policy)	Mixed
58	Unapproved	Banned By Policy	Mixed* (by Policy)	Mixed
59	Approved (by Policy)	Banned By Policy	Mixed* (by Policy)	Mixed
60	Banned (by Policy)	Banned By Policy	Mixed* (by Policy)	Mixed

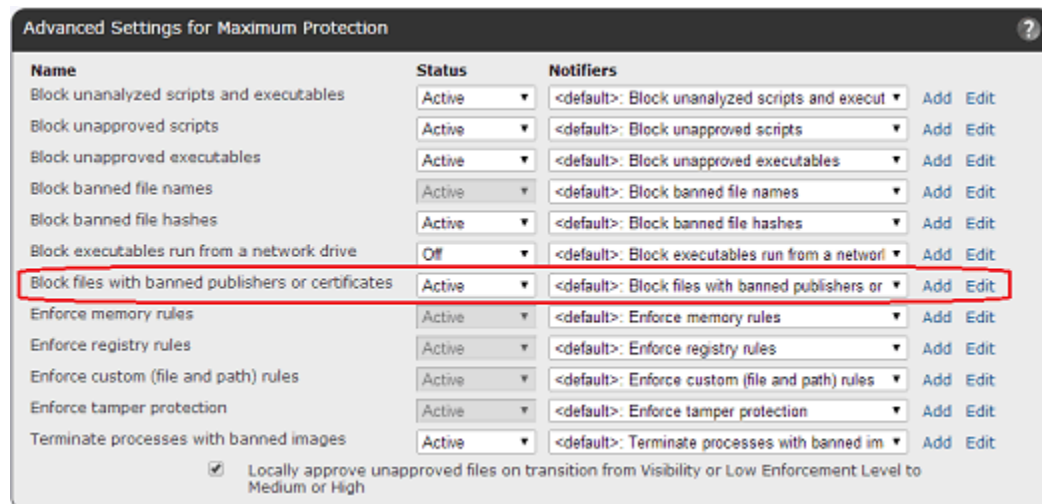
## Mixed and By-Policy States

As [Table 42](#) shows, Certificate Global State can be Mixed, Approved by Policy or Banned by Policy in certain cases. The table shows each case, but keep these general rules in mind:

- **Mixed Path State** – Certificate Path State is considered Mixed when some certificates are Approved and some are Banned. The Mixed state for path is strictly informational, however. In terms of its contribution to Certificate Global State, a Mixed path is equivalent to a Banned path.
- **By Policy Publisher State** – When a Publisher State is Banned by Policy or Approved by Policy, any ban or approval on a certificate in the path is filtered through the publisher policy choices. For example, if a certificate is Banned and it’s publisher is Approved by Policy, the Certificate Global Policy is Mixed.

## Certificate Ban Setting in Policies

The Advanced Settings panel for each policy includes a *Block files with banned publishers or certificates* setting. This setting must be Active (the default) for certificate bans to have affect file blocking. The certificate setting is effective only in High, Medium and Low Enforcement policies. Also, it affects only *enforcement* of certificate bans, not whether you can assign a ban to a certificate. Also, your choice here does not prevent any certificate from being *approved* or for an approval to be effective on a file.



## Interactions with Other Rules

Certificate Global State interacts with other rules and states to contribute to the state of a file. The configuration rules contributing to Certificate Global State were described “[Certificate Global State](#)” on page 308. The following are other rules of potential interest:

- **Enforcement Level** – If Certificate Global State is Banned, it can have an effect on whether files can be executed in High, Medium, and Low Enforcement Levels. If Certificate Global State is Approved, it can have an effect on file execution in High and Medium Enforcement Level.
- **Reputation Rules** – Reputation Rules can affect Publisher State, which can affect Certificate Global State. Keep this in mind if you have already assigned state to individual certificates and then enable or change Reputation Rules. See [Chapter 9](#), “[Reputation Approval Rules](#),” for more details.

## How Certificate Global State Affects Global File State

Global File State is a combination of File State, Publisher State, and Certificate Global State. If all certificates in a path are Unapproved, certificates do not contribute to Global File State. If a certificate has a Certificate Global State other than Unapproved, it can play a part in determining Global File State. The two simplest cases are:

- If there are no “by Policy” state settings, then if File State or Publisher State or Certificate Global State is Banned, Global File State is Banned.
- If there are no “by Policy” state settings, then if none of the three components contributing to Global File State is Banned and at least one is Approved, Global File State is Approved.

## Agent Version and Global File State

For agents at v7.0.1 Patch 3 and later, including all v7.2 agents, Global File State is effectively a combination of Certificate Global State and File State – Publisher State is already considered in the calculation of Certificate Global State.

For agents prior to v7.0.1 Patch 3, Global File State remains a combination of Publisher State and File State. Certificate Global State is not involved in Global File State determination.

See [Chapter 7, “File and Publisher Information,”](#) for more information on how Global File State is determined.

## Chapter 11

# Managing Devices

This chapter describes features for tracking and control of storage devices detected on computers running the Bit9 Agent.

**Sections**

Topic	Page
<a href="#">Overview</a>	316
<a href="#">Devices Managed by Bit9</a>	316
<a href="#">Enabling Per-Policy Device Control</a>	317
<a href="#">Managing Specific Devices</a>	320
<a href="#">Viewing Device Information</a>	320
<a href="#">Managing Devices by Model</a>	321
<a href="#">Managing Device Instances</a>	325
<a href="#">Managing Computer-Device Attachments</a>	330

## Overview

The Bit9 Security Platform enables you to track fixed and removable storage devices on agent-managed Windows computers, and to control file operations that users can perform on those removable devices. Bit9 device management consists of the following:

- **Policy-specific device control settings** determine whether Bit9 rules control write and execute operations on devices connected to computers in a policy, and whether this control applies to unapproved devices, banned devices, or both.
- **Device-specific rules** allow you to explicitly approve or ban specific removable devices, either by *model* or by *individual device*, so that files can be written or executed on approved devices while banned or unapproved devices may be restricted by your policy settings. The behavior of these approval and ban rules is similar to the behavior of file approvals and bans in the Bit9 Platform.
- **Device inventory** tables show each device discovered by a Bit9 Agent, and make it possible for you to implement the device-specific rules. This inventory includes a list of device models, a list of individual devices, and a list of unique *attachments* of an individual device and an individual computer. You can drilldown on any instance in these lists.

Throughout this chapter, the term *individual device* means one specific device that can only be attached to one computer at a time. Generally, this means a specific model plus a unique serial number (at least unique for that model).

### Platform Note

For release 7.2.1, device visibility and control features are available only for computers running *Windows*. Device management is not currently available on Mac or Linux computers.

## Devices Managed by Bit9

The Bit9 Agent can detect several different kinds of devices on Windows computers. In general, if a device has an identifiable file system, it is added to the Devices tables. How a detected device is managed depends upon whether it is identified as fixed or removable:

- **Fixed devices** are included in the device inventory, but they cannot be approved, banned, or blocked by Bit9 rules.
- **Removable devices** are included in the device inventory, and they can be approved, banned, and blocked by Bit9 rules.

Note that Bit9 must rely on the information provided by a device to determine whether it is fixed or removable, and there are some cases in which the information is incorrect.

Specific categories of devices detected by Bit9 Agents include:

- IDE Devices
- SATA Devices
- SCSI Devices
- USB Devices
- FireWire (IEEE 1394) Devices
- Serial Bus Protocol 2 Devices



- Floppy Disk Drives

The USB devices detected may include solid-state “stick”-type drives, CD/DVD drives, and media card readers. Note that for any drive with removable media, the drive itself, not the media it reads, appears in the devices table.

#### Note

In addition to the device settings and rules described here, you can create custom path rules that affect what a device can or can't do. See [“Specifying Devices in Paths in Windows Rules”](#) on page 347 in [Chapter 12, “Custom Software Rules,”](#) for more information.

## Enabling Per-Policy Device Control

For any of the device control features in the Bit9 Platform to be enabled, you must activate device control settings on policies. Each policy can have its own device control configuration. These settings allow you to activate blocking for any combination of the following:

- banned devices and/or unapproved devices
- write and/or execute operations

You cannot block read operations on devices, but you can enable reporting so that when a file is read on a banned or unapproved device, an event is generated.

You enable device control on the Edit Policy page for policies that have already been created. Device Control Settings do not appear on the Add Policy page for a new policy you are creating.

For policies in Visibility mode, you can choose any device control setting, but no device operations are blocked. To block device activity, a policy must be in Control mode.

#### Note

The effect of the settings on drives with removable *media*, such as CD/DVD drives, differs from the effect on devices with non-removable media. Burning a CD or DVD does not constitute a “Write” operation. If you want to block burning of CD/DVD media, ban the media-burning software application.

[Table 43](#) shows the effects of specific choices for Device Control settings.

**Table 43:** Device Control Setting Behavior

Setting	Active	Off	Report Only
<b>Block writes to unapproved removable devices</b>	Tracks write operations to unapproved removable devices and blocks them in all Control mode policies (High, Medium and Low Enforcement). <b>Notes:</b> <ul style="list-style-type: none"> <li>All devices are unapproved by default, so be certain you want to block everything you haven't explicitly approved before activating this setting.</li> <li>Blocking writes to removable devices does not block writes to CD/DVD media.</li> </ul>	Permits write operations to removable devices; does not report the event.	Permits write operations and reports them as events.
<b>Block writes to banned removable devices</b>	Tracks write operations to banned removable devices and blocks them in all Control mode policies (High, Medium and Low Enforcement). <b>Note:</b> Blocking writes to removable devices does not block writes to CD/DVD media.	Permits write operations to banned removable devices; does not report the event.	Permits write operations and reports them as events.
<b>Report reads from unapproved removable devices</b>	Choice not available.	Permits reads from unapproved removable devices; does not report the event.	Permits reads and reports them as events.
<b>Report reads from banned removable devices</b>	Choice not available.	Permits reads from banned removable devices; does not report the event.	Permits reads and reports them as events.
<b>Block execution from unapproved removable devices</b>	Tracks execution of files on unapproved removable devices and blocks them in all Control mode policies (High, Medium and Low Enforcement). <b>Note:</b> All devices are unapproved by default, so be certain you want to block everything you haven't explicitly approved before activating this setting.	Permits files on unapproved removable-device to execute unless the file itself is banned by another rule; does not report the event.	Permits executions and reports them as events.
<b>Block execution from banned devices</b>	Tracks execution of files on banned removable devices and blocks them in all Control mode policies (High, Medium and Low Enforcement).	Permits execution of files on banned removable-device unless the file is banned by another rule; does not report the event.	Permits executions and reports them as events.

In the Default, Template and Local Approval policies, device controls are all set to *Off* (no blocking or reporting) except for the settings that block writes and executions to banned devices, which are *Active*. You can change this for all except the Local Approval Policy. Changing the settings in the Template Policy *before* you create other policies can save time in policy configuration.

### To enable device control for a policy:

1. On the console menu, choose **Rules > Policies**. The Policies page opens.
2. On the Policies page, click the View Details (pencil and file) button next to the name of the policy whose device settings you want to edit. The Edit Policy page opens.

**Edit Policy Research Team**

Policy Name: Research Team  
 Description:

Mode:  Visibility  Control  Disabled

Enforcement Level: Connected: Medium (Prompt Unapproved) | Disconnected: Medium (Prompt Unapproved)

Notification Link:   
 Notification Logo:

Automatic Policy Assignment For New Computers:   
 Set Automatic Policy For Existing Computers: There are currently no computers in this policy.

Options:  Allow Upgrades  Track File Changes

---

**Device Control Settings for Research Team**

Name	Status	Notifiers
Block writes to unapproved removable devices	Off	<default>: Block writes to unap Add Edit
Block writes to banned removable devices	Active	<default>: Block writes to banr Add Edit
Report reads from unapproved removable devices	Off	<none>
Report reads from banned removable devices	Off	<none>
Block executions from unapproved removable devices	Off	<default>: Block executions fr Add Edit
Block executions from banned removable devices	Active	<default>: Block executions fr Add Edit

Save Cancel Reset Policy Show Advanced Settings

3. On the Device Control Settings panel, choose **Active** for any setting you want to enable, **Off** for any setting you want to disable, and **Report Only** for any setting for which you want the Bit9 Server to report file activity on devices but not enforce the setting. Note that you cannot block Read access to devices, so Active is not a choice for the two Read settings. See [Table 43, “Device Control Setting Behavior,”](#) on page 318 for details about the effects of each setting.
4. You can change (or eliminate) the notifier that appears when a device setting blocks file access. To do this, make a choice on the Notifier menu next to each setting whose notifier you want to change. See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for more options and more information.
5. When the Device Settings and their notifiers are edited to your preferences, click the **Save** button at the bottom of the Edit Policy page. Your changes are saved for that policy.
6. Repeat this procedure for each policy whose Device Settings you want to change.

## Managing Specific Devices

The Bit9 Security Platform collects many different kinds of information about the devices it detects on your computers. You can use this information to make decisions about how you want to treat file activities on devices.

By default, all devices are in an unapproved state (neither approved nor banned) . You can explicitly approve or ban specific removable devices, either by model or by serial number. Files not blocked by other rules are always allowed to execute and be written on approved devices. Treatment of unapproved and banned files varies depending upon the Device Control Settings for each policy.

### Note

Banned devices do not block in policies that are set to Visibility mode, but you can choose Report Only for the Device Settings to generate events for device-related activity that would have blocked in Control mode.

Similarly, device-specific bans and approvals do not block or allow access in policies that do not have Device Settings set to *Active*.

## Viewing Device Information

Device information is presented in table form on the Devices page, which you access by choosing **Assets > Devices** on the console menu. From each device table, you can drill down to a details page for any single item on the page (model, device instance, or attachment) by clicking on the View Details button (file and pencil) next to the item. The following table shows the type of information available in each of these views:

This Device information...	...is listed in this Table	...and this Details page for each Table row
Device Models found (vendor plus name)	Device Catalog ( <i>Show Individual devices</i> box <b>not</b> checked)	Device Model Details (for one model)
Individual Devices found (unique serial number)	Device Catalog ( <i>Show Individual devices</i> box <b>checked</b> )	Device Details (for one serial number)
Individual Devices attached to Individual Computers	Devices on Computers	Device Attachment Details (for one device-computer pair)

The Device tables do not have Saved Views, but the *Group By* menu allows you to group information by different fields. For example, you might want to see all of the devices grouped by *vendor*, or view all devices models for which certain serial numbers have rules that are an *exception* to the rule for the model. The Group By menu provides options for each of these cases. If you have not already become familiar with modifying views, see “[Bit9 Console Tables](#)” on page 58.

## Managing Devices by Model

You can monitor and manage devices attached to computers by their model. Managing devices by model provides a way to control many devices with a single rule. You can:

- View the full list of device models in the Device Catalog.
- View complete information about one device model on the Device Model Details page. You can view other information *related* to a device model by using the Related Views menu.
- Approve, ban, and remove approvals or bans from either the Device Catalog or the Device Model Details page.

## Viewing Device Models in the Device Catalog

Device models are identified as a specific pairing of vendor and product name. The Device Model table provides general information about the types of devices connected to your computers, and allows approving or banning all instances of a device model.

**To view all device models detected by Bit9:**

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Click on the **Device Catalog** tab. The Device Catalog table appears on the page.
3. Scroll to the bottom of the page, and if the *Show individual devices* checkbox is checked, click on it to remove the checkmark. The Device Catalog shows the table of device models.

Action	State	Exceptions	Vendor	Name	Device Class	First Seen Computer	Computer Count
State: Approved							4 items
<input type="checkbox"/>	Approved	No	HTC	Android Phone	USB Device	MYCORP\Laptop-2	7
<input type="checkbox"/>	Approved	No	Kingston	DataTraveler II	USB Device	MYCORP\Desktop-11	8
<input type="checkbox"/>	Approved	No	IronKey	IronKey	USB Device	MYCORP\Server-3	3
<input type="checkbox"/>	Approved	No	SanDisk Corp	U3 Cruzer Micro	USB Device	MYCORP\Laptop-5	5
State: Unapproved							99 items

See [Table 44, “Device Model Details,”](#) on page 323 for a description of the columns that can be displayed in this table.

The Action menu in the Device Catalog for models acts on checked table rows. It includes the following commands:

- Globally Approve
- Globally Ban
- Remove Approval or Ban
- Acknowledge

The approval and ban commands are described in “[Approving and Banning Device Models](#)” on page 324. You can use the Acknowledge command to indicate that you have reviewed a particular model and perhaps taken any action you intend to take on its status. You can then sort or filter the table so that device models you haven’t yet acknowledged are more visible.

## Viewing Details for One Device Model

The Device Model Details page provides information about the model. [Table 44, “Device Model Details,”](#) describes the fields shown on this page.

**Device Model Details**

**General**

Vendor: Maxtor  
 Name: OneTouch  
 Class: USB Device  
 Friendly Name:  
 Removable Device: Yes  
 Acknowledged: No  
 Description:  
 Device Count: There is 1 individual device for this model.  
 Computer Count: This device model was attached to 0 computer

**Rule**

State: Select the default state for this device model...  
 Unapproved  
 Approved Serial Numbers: Approve only serial numbers that match...  
 3LBPTPG3  
 Banned Serial Numbers: Ban only serial numbers that match...  
 Rule Applies To:  All policies  Selected policies

**History**

Dec 07 2011 03:20:58PM User admin changed the state to "Unapproved" and approved serial numbers that match: 3LBPTPG3 in policy: All Policies  
 Oct 07 2007 08:24:02AM This device model was first seen on MYCORP\Desktop-6

**Related Views**

- All devices of this model
- All computers with this device model
- All events for this device model

Save Cancel

The Device Model Details page is also where you configure the rule for how devices of this model should be treated. This is done on the page itself rather than on a menu. The rule includes the overall state of the model as well as any exceptions for specific serial numbers.

The Related Views menu provides links to the following information:

- **All devices of this model** – Filters the Device Catalog to show all instances of this device model that have been attached to agent-managed computers.
- **All computers with this device model** – Filters the Devices on Computers table to show all computers to which devices of this model have been attached.
- **All events for this device model** – Goes to the Events page and filters it to show all events related to this device model, including initial discovery of each instance and any time a device of this model has been attached or detached from a computer.

**Table 44:** Device Model Details

Field	Description
<b>Vendor</b>	The brand of the device (e.g., "SanDisk"). If the device does not have detectable vendor information, this field might show something like "USB DISK" or "Flash".
<b>Name</b>	The name of the device model, which might be a trade name (e.g., "Jumpdrive Pro") or a model number (e.g., "c30w"). If the device does not have detectable model name, this field might show something like "USB Storage Device" or "Unnamed Product".
<b>Class</b>	This is primarily a description of the interface for the device. The choices are IDE Device, SATA Device, SCSI Device, USB Device, FireWire (IEEE 1394) Device, Serial Bus Protocol 2, Floppy Disk, and Unknown.
<b>Removable Device</b>	Whether the device is removable or not removable. Values are <b>Yes</b> or <b>No</b> . Note that some devices might not provide accurate information for this field.
<b>Friendly Name</b>	The common name for this device, for example, as you would see it in Windows Explorer when the device is connected.
<b>Acknowledged*</b>	You may Acknowledge a device to indicate that you have seen it and perhaps do not need to track it as closely. Acknowledging a device does not change its approval state. The Action menu and a dropdown menu on the details page allow you to choose <b>Yes</b> or <b>No</b> for this field.
<b>Description</b>	Editable text providing any information you would like to include with the record of this device model.
<b>Device Count</b>	The number of unique devices (i.e., unique serial numbers) of this model detected by Bit9 on your computers.
<b>Computer Count</b>	The number of computers to which a device of this model has been attached.
<b>First Seen Platform</b>	The first platform (Windows, Mac, or Linux) on which this device model was seen. For release 7.2.1, this will always be Windows.
<b>State</b>	The default state for this device model. The choices are Approved, Banned, and Unapproved. Note that specific instances (serial numbers) of a device model can have a state that differs from the default model state.
<b>Approved Serial Numbers</b>	If the default state of the device model is Unapproved or Banned, you can specify serial numbers that are Approved. You can enter one or more specific serial numbers, or a pattern that uses wildcards to include a range of numbers.
<b>Banned Serial Numbers</b>	If the default state of the device model is Unapproved or Approved, you can specify serial numbers that are Banned. You can enter one or more specific serial numbers, or a pattern that uses wildcards to include a range of numbers.
<b>Rule Applies To</b>	You can make a device model rule apply to computers in all policies or only certain policies.
<b>History</b>	Records the date and time when the device was discovered and when rules affecting it were applied or changed.

## Approving and Banning Device Models

There are two options for managing device model approvals and bans:

- In the Device Catalog, you can check one or more device models in the table and use the Action menu to approve, ban, or remove the approval or ban for all of the checked items.
- On the Device Model Details page, you can approve, ban, or remove the approval or ban for the device model listed on the page. You also can view, add and delete exceptions (by serial number) to the default rule for the model, and you can make the rule apply to all policies or only certain policies.

### To approve one or more device models from the Device Catalog:

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Click on the Device Catalog tab, and in the lower right corner of the catalog page, make sure the *Show individual devices* box is *not* checked. The title of the table you see should say *Devices: Storage Device Catalog*.
3. Check the box next to each device model you want to approve and then choose **Globally Approve** on the Action menu.
4. Choose **OK** on the confirmation dialog. The device models will be approved, and all instances of the device model will be approved by default.

To ban one or more models, use the procedure above and substitute **Globally Ban** for the Action menu choice in Step 3.

To remove approvals or bans from one or more models, use the procedure above and substitute **Remove Approval or Ban** for the Action menu choice in Step 3.

### Notes

- Only devices identified as removable can be approved or banned. If any *fixed* devices are checked when you attempt to approve or ban models from the Device Catalog, you will see an error message and the non-removable drives will not be affected. If any *removable* devices are included in the selection, they will be affected by the command even if other devices are not. You can determine whether a device can be approved or banned by checking the *Removable Device* column in the table.
- All approval and ban actions taken from the Device Catalog are global, affecting all device instances and computers in all policies. If you want to limit an approval or ban to devices on computers in particular policies, or if you want to add exceptions to the rule for specific device serial numbers, use the Device Model Details page.
- You can select combinations of Banned and Approved models when you use the Remove Approval or Ban command – all will be moved to the Unapproved state.



**To approve one device model from the Device Model Details page:**

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Click on the Device Catalog tab, and in the lower right corner of the catalog page, make sure the *Show individual devices* box is *not* checked. The title of the table you see should say *Devices: Storage Device Catalog*.
3. Click on the View Details button (file and pencil) next to the device model you want to approve. The Device Model Details page appears.
4. If you want to limit this approval to certain policies, click the **Selected policies** radio button and check the boxes next to the policies you want enabled.
5. On the State menu, choose **Approved**.
6. If you want to ban certain instances of this device model even though you are approving the model itself, enter one or more serial numbers (or a serial number pattern with wildcards) into the *Banned Serial Numbers* field.

You also can add exceptions later by approving or banning device instances in the Device Catalog or Devices on Computers tables, or by using the approve or ban commands in the Device Instance Details or Device Attachment Details page.

7. Click the **Save** button at the bottom of the page and click **OK** on the confirmation dialog. The device model will be approved, and all instances except those you created exceptions for will be approved.

To ban a model from its details page, use the procedure above and choose **Banned** for the State menu choice in Step 5. If you want to create exceptions and you know their serial numbers, enter the numbers or a pattern to match in the *Approved Serial Numbers* field.

To remove a model approval or ban using the details page, use the procedure above and substitute **Unapproved** for the Action menu choice in Step 3.

**Note**

Only devices identified as removable can be approved or banned. Non-removable devices do not have a Rules section on the Device Model Details page.

## Managing Device Instances

You can monitor and manage individual devices, as identified by their serial number. Managing devices by instance provides a way to control specific devices for which you might want different treatment than others devices of the same model. You can:

- View the full list of device instances in the Device Catalog.
- View complete information about one device instance on the Device Details page. You also can see other information related to a device through Related Views.
- Approve, ban, and remove approvals or bans from either the Device Catalog or the Device Details page.

## Viewing Instances in the Device Catalog

A device instance is identified by its serial number, vendor and name. The device instance view can be useful for information about the number of devices on your computers, and for approving or banning specific device instances.

**To view all unique device instances detected by Bit9:**

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Click on the **Device Catalog** tab. The Device Catalog table appears on the page.
3. Scroll to the bottom of the page, and if the *Show individual devices* checkbox is not checked, click on it to *check* the box. The Device Catalog shows the table of device instances with unique serial numbers.

Devices: Individual Storage Devices

Device Catalog | Devices on Computers

Group By:  
State | Ascending

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Action	State	Vendor	Name	Device Class	Serial Number	First Seen Computer	Computer Count
<input type="checkbox"/>	Approved	HTC	Android Phone	USB Device	HT14ADK59246	MYCORP\Laptop-2	2
<input type="checkbox"/>	Approved	HTC	Android Phone	USB Device	HT09VJV21213	MYCORP\Desktop-1	1
<input type="checkbox"/>	Approved	HTC	Android Phone	USB Device	HT06THQ15645	MYCORP\Laptop-5	3
<input type="checkbox"/>	Approved	HTC	Android Phone	USB Device	HT12GHG23234	MYCORP\Desktop-11	1
<input type="checkbox"/>	Approved	IronKey	IronKey	USB Device	19074b03872511	MYCORP\Server-3	5

611 items Page 1/24 25 rows per page

Show individual devices

See [Table 45, “Device Details \(unique serial number\),”](#) on page 328 for a description of the columns that can be displayed in this table.

The Action menu in the Device Catalog for instances acts on checked table rows. It includes the following commands:

- Globally Approve
- Globally Ban
- Remove Approval or Ban
- Acknowledge

The approval and ban commands are described in [“Approving or Banning Device Instances”](#) on page 328. You can use the Acknowledge command to indicate that you have reviewed a particular device instance and perhaps taken any action you intend to take on its status. You can then sort or filter the table so that device models you have not yet acknowledged are more visible.

## Viewing Details for One Device Instance

The Devices Details page shows the information about one unique device (with a unique serial number). [Table 45, “Device Details \(unique serial number\),”](#) on page 328 describes the fields shown on this page.

The screenshot shows a 'Device Details' window with a 'General' tab. The main content area displays the following information:

Vendor:	TDKMedia
Name:	Trans-It Drive
Class:	USB Device
Friendly Name:	TDKMedia Trans-It Drive USB Device
Removable Device:	Yes
Serial Number:	25B704030AA69003
Default State:	Unapproved
Device State:	Approved
First Seen Computer:	MYCORP\Laptop-4
First Seen Date:	Oct 26 2011 05:18:23PM
Computer Count:	This individual device was attached to 4 computers.

Below the main content area is a 'Close' button. To the right of the main content area are two sections: 'Related Views' and 'Actions'. The 'Related Views' section contains three links: 'Model details', 'All computers with this device', and 'All events for this device'. The 'Actions' section contains two links: 'Ban Serial Number' and 'Approve Serial Number'.

The Device Details page includes an Actions menu and a Related Views menu.

The Actions menu includes commands for approving and banning this device, and for removing approvals or bans. The commands that appear depend on the current state of the device. See [“Approving or Banning Device Instances”](#) on page 328 for more information about using these commands.

The Related Views menu provides links to the following information:

- **Model details** – Goes to the Device Model Details page for this device, which shows both information about the model itself and the default rule definitions for the model.
- **All computers with this device** – Filters the Devices on Computers table to show all computers to which this device instance has been attached.
- **All events for this device** – Goes to the Events page and filters it to show all events related to this device instance (by serial number), including its initial discovery and the dates and times it has been attached or detached from a computer.

**Table 45:** Device Details (unique serial number)

Field	Description
<b>Vendor</b>	The brand of the device (e.g., "SanDisk"). If the device does not have detectable vendor information, this field might show something like "USB DISK" or "Flash".
<b>Name</b>	The name of the device model, which might be a trade name (e.g., "Jumpdrive Pro") or a model number (e.g., "c30w"). If the device does not have detectable model name, this field might show something like "USB Storage Device" or "Unnamed Product".
<b>Class</b>	This is primarily a description of the interface for the device. The choices are IDE Device, SATA Device, SCSI Device, USB Device, FireWire (IEEE 1394) Device, Serial Bus Protocol 2, Floppy Disk, and Unknown.
<b>Removable Device</b>	Whether the device is removable or not removable. Values are <b>Yes</b> or <b>No</b> . Note that some devices might not provide accurate information for this field.
<b>Friendly Name</b>	The common name for this device, for example, as you would see it in Windows Explorer when the device is connected. This is often some combination or variant of the Vendor and Name.
<b>Serial Number</b>	The serial number that identifies this unique individual device.
<b>Default State</b>	The default state for this device (which is the state for its <i>model</i> ). The choices are Approved, Banned, and Unapproved. Note that this specific instance might have a state that differs from the default.
<b>Device State</b>	The actual state for this individual device (as identified by serial number). The choices are Approved, Banned, and Unapproved.
<b>First Seen Computer</b>	The computer on which this individual device was first detected by a Bit9 Agent.
<b>Platform</b>	Platform (Windows, Mac, or Linux) of the computer on which the device was first detected. For release 7.2.1, this will always be Windows.
<b>First Seen Date</b>	The date and time when this individual device was first detected by a Bit9 Agent.
<b>Computer Count</b>	The number of different computers to which this individual device has been connected.

## Approving or Banning Device Instances

There are two options for managing device instance (serial number) approvals and bans:

- In the Device Catalog or Devices on Computers page, you can check one or more device instances in the table and use the Action menu to approve, ban, or remove the approval or ban, for all of the checked items.
- On the Device Details page or Device Attachment Details page, you can approve, ban, or remove the approval or ban for the device instance listed on the page.

You only need to approve, ban, or remove approvals or bans from an instance if you want it to have a state other than the default state for its device model. Instance-specific

exceptions appear on the Device Model Details page for the device model.

**To approve one or more device instances from the Device Catalog:**

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Either:
  - Click on the **Device Catalog** tab, and in the lower right corner of the catalog page, make sure the *Show individual devices* box is checked. The title of the table you see should say *Devices: Individual Storage Devices*.
  - **- or -**
  - Click on the **Devices on Computers** tab.
3. Check the box next to each device instance you want to approve and then choose **Globally Approve** on the Action menu.
4. Choose **OK** on the confirmation dialog. The device will be approved by serial number.

To ban one or more instances, use the procedure above and substitute **Globally Ban** for the Action menu choice in Step 3.

To remove approvals or bans from one or more instances, use the procedure above and substitute **Remove Approval or Ban** for the Action menu choice in Step 3.

**Notes**

- Only devices identified as removable can be approved or banned. If any *fixed* devices are checked when you attempt to approve or ban devices, you will see an error message and the non-removable drives will not be affected. If any *removable* devices are included in the selection, they will be affected by the command even if other devices are not. You can determine whether a device can be approved or banned by checking the *Removable* column in the table.
- All approval and ban actions taken on device *instances* become exceptions within the rule for their device *model*, and are applied to all policies or selected policies as specified in the model rule.
- You can select combinations of Banned and Approved devices when you use the Remove Approval or Ban command – all will be moved to the Unapproved state.

**To approve an instance from the Device Details or Device Attachment Details page:**

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Either:
  - Click on the **Device Catalog** tab, and in the lower right corner of the catalog page, make sure the *Show individual devices* box is checked. The title of the table you see should say *Devices: Individual Storage Devices*.
  - **- or -**
  - Click on the **Devices on Computers** tab.

3. Click on the View Details button (file and pencil) next to the device instance you want to approve. The Device Details or Device Attachment Details page appears.
4. In the Actions menu on the right side of the page, choose **Approve Serial Number**. The device will be approved, and its serial number will be added as an exception on the Device Model Details page for its model.

To ban a device instance from its details page, use the procedure above and substitute **Ban Serial Number** as the Actions menu choice in Step 4.

To remove a device instance approval or ban using the details page, use the procedure and substitute the appropriate removal command.

#### Note

Only devices identified as removable can be approved or banned. If you attempt to approve or ban a fixed device, you will see an error message.

## Managing Computer-Device Attachments

You can monitor attachments between a specific device instance and a specific computer, and manage the individual devices. You can:

- View the full list of device-computer attachments in the Devices on Computers table.
- View complete information about an attachment between one specific device and one specific computer on the Device Attachment Details page. You also can see other information related to this attachment or the individual device through Related Views.
- Approve, ban, and remove approvals or bans from either the Devices on Computers table or the Device Attachment Details page.

## Viewing Devices on Computers

The Devices on Computers tab provides a table of individual devices that have been connected to individual computers. The relationship between one device and one computer counts as a single “attachment” in the table, regardless of how many times the two have been connected and disconnected. If you are concerned about the use of removable devices on a particular computer, the Devices on Computers page provides a way to find out if any such connections exist. You can approve and ban individual devices from this table.

**To view all attachments between a specific device and a specific computer:**

1. On the console menu, choose **Assets > Devices**. The Devices page appears.
2. Click on the **Devices on Computers** tab. The Devices on Computers page appears, listing each pairing of a device instance (with a unique serial number) and a specific computer.

	State	Vendor	Name	Serial Number	Device Class	Computer Name	Attached
<input type="checkbox"/>	Unapproved	HTC	Android Phone	45672908C099	USB Device	MYCORP\Laptop-12	Yes
<input type="checkbox"/>	Unapproved	Kingston	DataTraveler 2.0	23487A7048D8761F85	USB Device	MYCORP\Laptop-12	Yes
<input type="checkbox"/>	Unapproved	ADATA	SSD_5599_128G	588200D3018081.0.0	IDE Device	MYCORP\Server-3	No
<input type="checkbox"/>	Unapproved	Apple Inc.	iPod	000A27001A9ABEB0	USB Device	MYCORP\Laptop-12	No

See [Table 46, “Device Attachment Details,”](#) on page 333 for a description of the columns that can be displayed in this table.

The Action menu in the Devices on Computers table instances acts on checked table rows. It includes the following commands:

- Globally Approve
- Globally Ban
- Remove Approval or Ban
- Acknowledge

The approval and ban commands on both the Devices on Computers table and the Device Catalog for *instances* affect the instance, as defined by serial number, in the checked rows. You are not approving or banning a particular *attachment*. See [“Approving or Banning Device Instances”](#) on page 328 for more details.

You can use the Acknowledge command to indicate that you have reviewed a particular device instance and perhaps taken any action you intend to take on its status. You can then sort or filter the table so that device models you have not yet acknowledged are more visible.

## Viewing Details for One Computer-Device Attachment

The Devices Attachment Details page shows information about the history of attachment between one device instance and one computer. [Table 46, “Device Attachment Details,”](#) on page [333](#) describes the fields shown on this page.

The screenshot shows a window titled "Device Attachment Details" with a "General" tab. The main content area displays the following information:

<b>Vendor:</b>	SanDisk
<b>Name:</b>	SanDisk Cruzer
<b>Class:</b>	USB Device
<b>Friendly Name:</b>	SanDisk SanDisk Cruzer USB Device
<b>Removable Device:</b>	Yes
<b>Serial Number:</b>	10A2891620517373
<b>Default State:</b>	Unapproved
<b>Device State:</b>	Unapproved
<b>Computer:</b>	MYCORP\Desktop-15
<b>Platform:</b>	Windows
<b>Current Status:</b>	Detached
<b>First Attach Date:</b>	Dec 05 2011 10:20:11AM
<b>Last Attach Date:</b>	Dec 06 2011 02:14:47PM
<b>Last Detach Date:</b>	Dec 06 2011 04:03:11PM
<b>Computer Count:</b>	This individual device was attached to 1 computer.

On the right side of the window, there are two sections:

- Related Views:**
  - Model details
  - All computers with this device
  - All events for this device
- Actions:**
  - Ban Serial Number
  - Approve Serial Number

At the bottom left of the window is a "Close" button.

The Device Attachment Details page includes an Action menu and a Related Views menu.

The Action menu includes commands for approving and banning this device instance, and for removing approvals and bans. The commands that appear depend on the current state of the device. See [“Approving or Banning Device Instances”](#) on page [328](#) for more information about using these commands.

The Related Views menu provides links to the following information:

- **Model details** – Goes to the Device Model Details page for this device, which shows both information about the model itself and the default rule definitions for the model.
- **All computers with this device** – Filters the Devices on Computers table to show all computers to which this device instance has been attached.
- **All events for this device** – Goes to the Events page and filters it to show all events related to this device instance (by serial number) *on this computer*, including its initial discovery and any time it has been attached or detached from a computer.



**Table 46:** Device Attachment Details

Field	Description
<b>Vendor</b>	The brand of the device (e.g., "SanDisk"). If the device does not have detectable vendor information, this field might show something like "USB DISK" or "Flash".
<b>Name</b>	The name of the device model, which might be a trade name (e.g., "Jumpdrive Pro") or a model number (e.g., "c30w"). If the device does not have detectable model name, this field might show something like "USB Mass Storage Device" or "Unnamed Product".
<b>Class</b>	This is primarily a description of the interface for the device. The choices are IDE Device, SATA Device, SCSI Device, USB Device, FireWire (IEEE 1394) Device, Serial Bus Protocol 2, Floppy Disk, and Unknown.
<b>Removable Device</b>	Whether the device is removable or not removable. Values are <b>Yes</b> or <b>No</b> . Note that some devices might not provide accurate information for this field.
<b>Friendly Name</b>	The common name for this device, for example, as you would see it in Windows Explorer when the device is connected. This is often some combination or variant of the Vendor and Name.
<b>Serial Number</b>	The serial number that identifies the unique individual device that was attached to a computer.
<b>Default State</b>	The default state for this device model. The choices are Approved, Banned, and Unapproved. Note that this specific instance might have a state that differs from the default for the model.
<b>Device State</b>	The actual state for this individual device (as identified by serial number). The choices are Approved, Banned, and Unapproved.
<b>Computer</b>	The name of the computer to which the device was attached.
<b>Platform</b>	Platform (Windows, Mac, or Linux) of the computer to which the device was attached. For release 7.2.1, this will always be Windows.
<b>Current Status</b>	Whether the device and computer that define this attachment are currently Attached or Detached. <b>Note:</b> Device attachment status for computers disconnected from the Bit9 Server is the last known status when the computer was connected.
<b>First Attach Date</b>	The date and time when the device and computer were first attached.
<b>Last Attach Date</b>	The date and time when the device and computer were last attached.
<b>Last Detach Date</b>	The date and time when the device was last detached from the computer.
<b>Computer Count</b>	The number of different computers to which this individual device (as identified by serial number) has been attached.



## Chapter 12

# Custom Software Rules

This chapter describes Custom Rules, which provide special treatment of files matching paths you specify. Custom Rules may be used for performance optimizations, file integrity control, creation of a trusted file path for software distribution, and other special situations. They can be used to create exceptions to other rules, such as approvals or bans.

### Notes

Standard methods for approving and banning files are described in [Chapter 8, “Approving and Banning Software.”](#)

The Bit9 Security Platform provides these other rule types:

- See [Chapter 13, “Script Rules,”](#) for rules that add or modify definitions of scripts.
- See [Chapter 14, “Registry Rules,”](#) for rules that protect the Windows registry.
- See [Chapter 15, “Memory Rules,”](#) for rules that protect running processes from being accessed or altered by other processes.
- See [Chapter 16, “Event Rules,”](#) for rules that take actions, including approving or banning files, when certain events occur.

### Sections

Topic	Page
<a href="#">Overview</a>	336
<a href="#">Creating a Custom Rule</a>	338
<a href="#">Custom Rule Parameters</a>	341
<a href="#">Specifying Paths and Processes</a>	345
<a href="#">Rule Ranking</a>	354
<a href="#">Rule Ranking and Internal Rules</a>	356
<a href="#">Disabling or Deleting Custom Rules</a>	357
<a href="#">Exporting and Importing Rules</a>	359
<a href="#">Custom Rule Types and Examples</a>	366

## Overview

Custom rules provide special treatment of files matching file paths you specify. They specify that file executions or file write operations are to be treated in specific ways, including being blocked, permitted, reported on, or ignored, if they match the path description and other rule parameters.

## Rule Types

The Bit9 Security Platform provides several custom rule types partially configured for specific purposes:

- **File Integrity Control** – Prevents or reports changes to specified folders or files.
- **Trusted Path** – Defines folders or files for which file execution is always allowed.
- **Execution Control** – Creates a rule to control behavior when an attempt is made to *execute* a file matching the rule.
- **File Creation Control** – Creates a rule to control behavior when an attempt is made to *write* a file matching the rule.
- **Performance Optimization** – Specifies folders or files for which file creation, modification, and deletion are ignored (execution will still be monitored).

You also can choose an **Advanced** rule type in which you set all parameters yourself.

Custom rules can be used to enable network login scripts or software deployment systems, or to designate an area for software developers to run executables without the Bit9 Server tracking file activity or enforcing rules. You also can use a custom rule to prevent users from uninstalling an application by blocking any changes to that application's directory.

## Rule Scope

You can create custom rules that apply on all computers on a platform (e.g., all Windows computers) under all conditions, or you can focus the scope of a rule by specifying one or more of the following criteria (not all of these options are available for all rule types):

- **Process-specific** – You can choose to make a rule effective only when certain *processes* attempt to write or execute files in the specified location.
- **User- or group-specific** – You can make the rule apply only to a specific *user or group of users*.
- **Policy-specific** – You can choose to limit a rule to *computers in specified policies*.
- **Rule ranking** – Custom rules are evaluated in order of *Rank*, a column that is displayed by default on the Custom Rules table. The rule ranked '1' has the highest rank, '2' is next, and so on. With one exception (rules that ignore file writes), only the first rule matching a file is evaluated. You can change the order of rules, for example, putting a rule applying to *one specific file in a folder* higher on the list, while putting another rule for *all the files in the same folder* lower – because the first rule is higher, it takes precedence.

All user-created custom rules are platform-specific; that is, they apply to only one of the platforms – Windows, Mac, or Linux – that Bit9 Agents can be installed on.

## File and Process Matching

To determine whether a file or process attempting an action matches a custom rule, a string comparison is done between the file or process name and the specifications in the rule. Hash values are not used for custom rule processing.

You can include *wildcards* and special *macros* in a path or process specification to broaden the rule scope or allow the rule to match files or processes in locations that vary from one agent computer to another. See [“Specifying Paths and Processes”](#) on page 345 for additional details.

## Pre-configured Rules

A new installation of the Bit9 Server is pre-configured with several custom rules found to improve performance and/or prevent unnecessary tracking. These rules are enabled by default. You can remove or disable them if you choose. For Bit9 Security Platform upgrades, these rules are added *below* (i.e., with a lower rank than) rules that already existed.

The table of rules also includes rules labeled **[Sample]**, which are disabled by default. In general, these are application-specific rules that allow files needed for certain common applications or suites to be executed or written. You may enable these, with or without modifications of your own.

## Internal Rules in the Custom Rule Table

The Custom Rules table includes rules labeled *Internal*. These are the rules you enable in other parts of the console, mostly in the Device and Advanced Settings on the Edit Policy page. For example, *Block banned file hashes*, which is on the Advanced Settings table for a policy, is listed as an Internal rule on the Custom Rules page.

An internal rule shows its status as Enabled in the rules table if it is enabled in *any* policy. You cannot enable, disable, modify or move Internal Rules in the Custom Rules table, but you can move other, non-internal Custom Rules, relative to the Internal Rules to better control how and when different rules are enforced. See [“Rule Ranking and Internal Rules”](#) on page 356 for more details.

Internal rules are the only custom rules that apply to all platforms.

## Specifying the Notifier for a Custom Rule

The Bit9 Security Platform provides *notifiers* that can be displayed when a rule blocks an action or prompts the user for a decision to allow or block an action. For each custom rule, you can choose from two sources for the notifier:

- **Use Policy Specific Notifier** – Each Policy includes an Advanced Setting, “Enable custom (file and path) rules”, which is always on. This policy setting has a Notifier field in which you can specify the notifier that appears on agent computers when custom rules block an action. The policy setting also allows the choice of <none> to have no notifier for custom rules in that policy. You can assign the policy-specific custom rule notifier to any custom rule. See [“Advanced Settings”](#) on page 156 for more information.
- **Custom Notifier** – If you do not choose the policy-specific notifier, you can choose (or create) a notifier specifically for a custom rule. The choices appear on a menu on the Add/Edit Custom Rule page.

See [Table 47](#) below for the custom rule notifier settings. See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for more on notifiers.

When you choose Prompt as the rule action, Custom Notifier menu does not include <none> as an option because a prompt rule requires a notifier to appear.

When you choose Block as the rule action, you can choose <none> on the Custom Write Notifier menu since it is possible you want the rule to block actions without notification.

If you choose Use Policy Specific Notifier for a rule, it is possible that the policy specifies <none> as the Notifier for Enforce custom (file and path) rules. In this case, a notifier will not be shown, even for a Prompt rule. Unless you are certain that you never want to prompt the user for a response to a rule, choosing <none> for the custom rule notifier in a policy is not recommended.

## Custom Rules in Visibility Mode

In Visibility mode policies, the effect of custom rules depends on the type of rule:

- Custom rules that would block a file have no effect in Visibility mode, although they still generate Bit9 events.
- Custom rules that approve a file *do* change the file state, but in Visibility mode this has no effect on file execution.
- Custom rules that specify “Ignore” on the Write menu (see below) *are* effective in Visibility mode.

## Creating a Custom Rule

To create a custom rule from scratch, you would need to provide the information shown in bold in the left column:

General Description	Field on Add/Edit Custom Rule Page
If <b>this/these source process(es)</b> ...	Process
...and/or <b>this/these user(s)</b> ...	User or Group
... attempts to perform <b>this/these operation(s)</b> ...	Operation (Execute, Write or Both)
... on <b>this/these file(s)</b> ...	Path or File
... on computers in <b>this/these policy(ies)</b> ...	Rule applies to:
... on computers running on <b>this platform</b> ...	Platform
... then <b>this/these action (s)</b> should be taken.	Execute Action and/or Write Action

Except for platform, there could be multiple matching items for these parameters, or the rule could specify all items in that class (for example, the rule applies to all users, or all policies, or all source processes). Also, instead of the descriptions above, you could choose to have the rule function when any process *except* the ones you specify attempts the action, or the action is attempted on any file *except* the ones you specify.

On the Add Custom Rule page, your choice of *Rule Type* modifies other parameters so that you might not have to provide all of the information to define a rule:

- Some *fields* are eliminated from the page if they are not relevant (or have only one sensible value) for the rule type you choose.
- Some *menu choices* are eliminated so that only choices relevant to the rule type are available.
- *Inline Help text* changes on the Add Custom Rule to assist you in choosing values appropriate to this rule type for each configurable field.

**To add (create) a custom rule:**

1. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. On the Software Rules page, click the **Custom** tab. The Custom Rules table appears:

Rank	Status	Platform	Rule Type	Name	Action
1	Enabled	Mac	Performance Optimization	Ignore Installer Trash Cleanup	Ignore writes
2	Enabled	Mac	Performance Optimization	Ignore Finder Archive Temp	Ignore writes
3	Enabled	Mac	Performance Optimization	Ignore Time Machine Volume	Ignore writes
4	Enabled	Mac	Performance Optimization	Ignore Bootcamp Volume	Ignore writes
5	Enabled	Mac	File Creation Control	SUHelperD	Approve writes
6	Enabled	Mac	Advanced	MDWorker	Silence writes
7	Enabled	Mac	Advanced	MDS	Silence writes
8	Disabled	Mac	Performance Optimization	[Sample] Xcode - Ignore Intermediate Files	Ignore writes
9	Disabled	Mac	Execution Control	[Sample] Xcode Promote	Promote executes

3. Click the **Add Custom Rule** button. The Add Custom Rule page appears.

4. In the Name field, enter the name with which you want to identify this rule.
5. If you want to add other comments about the rule, such as its purpose or its relationship to other rules, you may provide an optional Description.
6. By default, a new custom rule is **Enabled** as soon as you define it and click **Save**. If do not want the rule to take effect immediately, click **Disabled** in the Status field.
7. Choose the Rule Type from the menu. File Integrity Control is the default choice. Specific rule types are partially configured for you. If none of the specific types appears to fit your needs, choose **Advanced** on the Rule Type menu to see the greatest number of configuration options. [Table 47](#) describes the different rule types as well as all of the other custom rule parameters.
8. Enter the remaining parameters you want for this custom rule (see [Table 47](#)) and then click the **Save** button. The newly created rule is listed at the *top* of the Custom Rules table.
9. If you do not want this rule to have top priority, use the arrows in the Rank column to move it down to the desired rank. See [“Rule Ranking”](#) on page 354 for more details.



## Custom Rule Parameters

Table 47 shows the parameters available on the Add/Edit Custom Rule page.

**Table 47:** Custom Rule Parameters

Field	Description
<b>Name</b>	Name by which this rule is identified. (Required)
<b>Description</b>	Additional information about the custom rule. This can be any text you choose to enter. (Optional)
<b>Status</b>	Radio buttons that make this rule Enabled or Disabled. This allows you to create a rule that you use only at certain times, or to temporarily disable a rule without losing its definition.
<b>Platform</b>	Platform (Windows, Mac, or Linux) for which this rule is effective. Except for built-in “internal” rules, each custom rule is specific to a single platform.
<b>Rule Type</b>	The Rule Type choice changes other options and defaults on the Add/Edit Custom Rule page to partially pre-configure rules for certain common scenarios. Options are <b>File Integrity Control</b> , <b>Trusted Path</b> , <b>Execution Control</b> , <b>File Creation Control</b> , <b>Performance Optimization</b> , and <b>Advanced</b> . See “ <a href="#">Custom Rule Types and Examples</a> ” on page 366 for descriptions and examples.
<b>Operation</b>	The type of operation the rule affects. The menu choices are <b>Execute</b> , <b>Write</b> , or <b>Execute and Write</b> .
<b>Execute Action</b>	The action to take when there is a file execution attempt matching this rule. The menu appears when the Operation choice is <i>Execute</i> or <i>Execute and Write</i> . See <a href="#">Table 48</a> for options.
<b>Write Action</b>	The action to take when there is an attempt to create, modify or delete a file matching this rule. The menu appears when Operation choice is <i>Write</i> or <i>Execute and Write</i> . See <a href="#">Table 49</a> for options.
<b>Use Policy Specific Notifier</b>	If you choose Block or Prompt as the Action, this checkbox appears to the right of the Action choice and is checked by default. If the box is checked, when a custom rule blocks an action, the notifier that appears is the one specified for the Enable Custom (file and path) Rules setting in the policy for the computer on which the action was blocked. If not checked, you can choose a custom notifier from the Custom Notifier menu.
<b>Custom Execute/Write Notifier</b>	If you choose Block or Prompt as the Action, and check the Use Policy Specific Notifier box, this menu appears. When Block is the Action, you can choose any notifier from the menu. The menu also includes a <none> option so that you can disable the notifier for this rule. When Prompt is the Action, you can choose any notifier on the menu. However, Prompt rules <i>must</i> display a notifier, so there is no <none> choice in this case.
<b>Path or File</b>	Path to which this rule applies. This can be a folder or a specific file. You can use a local path or a UNC path, but not mapped drives (for example, Z:\application). See “ <a href="#">Specifying Paths and Processes</a> ” on page 345 for details on specifying a path.

Field	Description
<b>Process</b>	This menu allows you to limit the rule so that it is applied only when certain processes attempt to execute or write files matching the path specification. See <a href="#">“Specifying Paths and Processes”</a> on page 345 for details on specifying a process and <a href="#">Table 51</a> for process menu options.
<b>User or Group</b>	The users or groups to which this rule applies. See <a href="#">“Specifying Users or Groups”</a> on page 353 for details on specifying users or groups.
<b>Rule applies to</b>	The radio buttons allow you to apply the rule to <b>All policies</b> or <b>Selected policies</b> . If you choose <b>Selected policies</b> , a list of all policies on your Bit9 Server appears, each with a checkbox.
<b>History</b>	For existing rules, a History panel appears showing when and by whom the rule was created and last modified.

## Specifying Execute and Write Actions

You can control two types of action with a custom rule: Execute Action and Write Action.

Execute Action is the action you want to take when there is a file execution attempt matching a rule. The Execute Action menu appears when the Operation choice is *Execute* or *Execute and Write*. [Table 48](#) shows the choices.

**Table 48:** Execute Action Choices

Menu Choice	Description
<b>Default</b>	Apply existing policy settings and other non-custom rules to file execution attempts matching this rule, <i>and do not process other custom rules</i> .
<b>Allow</b>	Allow a file matching the rule to execute in the specified path, even if execution would otherwise be blocked.  <b>Note:</b> The promotion state (whether the file is treated as an installer) depends on the process attempting the action (e.g., if that process is promoted, the newly created process will also be promoted).
<b>Block</b>	Prevent a file matching the rule from executing. When Block is chosen, the Use Policy Specific Notifier checkbox appears and is checked by default. You also can uncheck this box to choose a Custom Notifier to alert the user when the rule blocks an action. See <a href="#">Table 47</a> for more details.
<b>Promote</b>	Promote (treat as an installer) a file matching this rule. Even if a file is promoted, whether it can <i>run</i> or not depends on its existing file state and the Enforcement Level of the machine on which the execution is attempted. If the file is allowed to run, any files written by it will be locally approved unless already banned, and the written files also will be promoted if the process that wrote them attempts to execute them.

Menu Choice	Description
<b>Allow and Promote</b>	Allow a file matching the Path or File specification to execute regardless of its state, and promote it (treat it as an installer). Files written by a file matching an Allow and Promote rule will be locally approved unless already banned. See the section <a href="#">"Trusted Paths"</a> for more on choosing to trust execution of files by path name.
<b>Prompt</b>	<p>Display a notifier dialog to users when an attempt is made to execute a file matching this rule.</p> <p>When Prompt is chosen, the Use Policy Specific Notifier checkbox appears and is checked by default. You also can uncheck this box to choose a Custom Notifier to alert the user when the rule blocks an action. See <a href="#">Table 47</a> for more details.</p> <p>The user can Block execution, Allow execution (and locally approve the file if allowed), or Promote (and allow execution of) the file. The behavior for the choice the user makes is the same as the behavior if the rule itself specified Block, Allow, or Allow and Promote. If the user chooses Allow or Promote, subsequent actions that are identical to the one Allowed or Promoted are completed without prompting.</p> <p><b>Note:</b> Blocking or allowing execution from a Custom Rule prompt does not change the global approval or ban state.</p>
<b>Report</b>	Report (as an event) execution of a file matching this rule, regardless of file state.
<b>Report Process Create</b>	Report (as an event) creation of a process matching the file and path specified by this rule by the process specified by the rule.
<b>Block Silently</b>	Prevent execution of a file when the execution conditions match this rule. Do not display a notifier, and do not generate a Bit9 event.
<b>Report Process Exit</b>	Report (as an event) the exit of a process matching the file and path specified by this rule that was started by the process specified in the rule.
<b>Report Image Load</b>	Report (as an event) loading of a DLL or EXE matching the file and path specified by this rule when loaded by the process specified in the rule.

Write Action is the action to take when there is an attempt to create, modify or delete a file matching a rule. The Write Action menu appears on the Add/Edit Custom Rule page when Operation choice is *Write* or *Execute and Write*. [Table 49](#) shows the choices.

**Table 49:** Write Action Choices

Menu Choice	Description
<b>Silence</b>	For an action that matches this rule and one or more additional rules (built-in or user-created), prevent notifications, meters, and events without preventing enforcement of the other matching rule(s) For example, if another rule would ban or block an action, the ban or block is still effective. If an action matching a Silence rule would have displayed a prompt (allow or block) notifier, the action will be blocked. Available for Advanced rule types only.
<b>Default</b>	Apply existing policy settings and non-custom rules when an attempt is made to write a file matching this rule. <i>Do not process any other Custom Rules for matching files.</i>
<b>Ignore</b>	Do not track creation, modification or deletion of a file matching this rule. Although not tracked, files matching an ignore rule are still blocked from writing if the file state and Enforcement Level would normally enforce a block.  Ignore does not stop rule processing. If a write attempt matches an ignore rule and a rule lower in rank, the second rule <i>is</i> processed.
<b>Track</b>	Track creation, modification or deletion of a file matching this rule. This action allows creation of exceptions to Ignore rules. Appears only for Advanced rule types.
<b>Block</b>	Prevent writing of a file matching this rule. This prevents file creations, file deletions and file modifications.  When Block is chosen, the Use Policy Specific Notifier checkbox appears and is checked by default. You also can uncheck this box to choose a Custom Notifier to alert the user when the rule blocks an action. See <a href="#">Table 47</a> for more details.
<b>Approve</b>	Allow a file matching this rule to be created (written) and locally approve it <i>if possible</i> (if it is not banned globally or by policy).
<b>Approve as Installer</b>	Allow a file matching this rule to be created (written) in the named directory, and locally approve and mark it as an installer <i>if possible</i> (i.e., if it is not banned globally or by policy).  <b>Note:</b> “Approve as installer” by a custom rule is a local and transient action only. It has no impact on any other instance of the file, and is not effective on this instance if the file is globally flagged as “Not an installer” because the initial state was overridden. The rule <i>is</i> effective if a file is marked as “Not an installer” because of the initial Bit9 analysis of the file.  Use this option with caution since it allows a file to be identified by <i>name</i> as an installer without confirming the file hash.
<b>Prompt</b>	Present users who attempt to write a file matching the rule with a notifier dialog letting them block or allow writing.  When Prompt is chosen, the Use Policy Specific Notifier checkbox appears and is checked by default. You also can uncheck this box to choose a Custom Notifier to alert the user when the rule blocks an action. See <a href="#">Table 47</a> for more details  If the user selects Approve on the notifier, the file is written, and if it is an executable, it is approved. Subsequent identical operations (i.e., the same file and path, not a different matching file) are approved without prompting. Note, however, that global bans by name or hash still control whether the file can be executed.

Menu Choice	Description
<b>Allow</b>	Allow a file matching this rule to be created, modified, or deleted. This choice has no effect on the state of the file being written.
<b>Report</b>	Report (as an event) writing of <i>any</i> file matching this rule, even if the file is not normally tracked by the Bit9 Server. This includes files not analyzed as executable and files that are not the first seen instance of a hash.
<b>Never Report</b>	Never report actions matching this rule to the server. A record of the action will still be maintained on the agent.

## Specifying Paths and Processes

When you specify Path or File in a Custom Rule, you have several options for defining the string for that parameter. These same options can be used when you choose one of the two Process options that require entry of a path (*Specific Process...* or *Any Process Except ...*).

These options are:

- **Specify a directory or a file/process** – You can enter a path or process specification that exactly identifies a file by path and name so that only that file matches the rule. You also can enter a specification that identifies a directory, and so affects all files or processes in that directory and its subdirectories.
- **Specify a local drive or UNC path (Windows only)** – You can use a local drive name, such as *C:\folder\subfolder\application.exe*, to identify a local path or process. For a remote path or process, use a UNC path, such as *\\computer\dir\application.exe*. Mapped drives in a path or process specification are not recognized.
- **Use wildcards** – You can use wildcards (“?” for any one character and “\*” for zero or more characters) to expand the scope of a path or process specification, or to help you match a file or folder whose exact location you don’t know. Wildcards may be used at the beginning, end or middle of a path.
- **Use macros** – You can use special macros to identify certain well known folders, even if you don’t know their exact location on agent computers. Macros are platform-specific, and in the current release, available only for Windows.
- **Specify multiple paths or processes** – For both paths and processes, you can add more than one path definition per rule.

## Specifying a File or Directory

You can enter a directory or a specific file as your path. When you specify a directory, you are instructing the rule to operate on files in that directory and any of its subdirectories (unless there are higher-ranked rules specific to certain files or subdirectories).

To indicate that a Path or File definition or a Process definition is a directory, you must end it with the folder delimiter (slash or backslash) for the rule platform or with the delimiter and an asterisk. If you do not include the delimiter, the rule will attempt to match a *file* by the name you provided, not a directory. For example, either of the following correctly identifies a directory in a Windows path definition:

```
c:\folder1\subfolder2\  
c:\folder1\subfolder2\*
```

However, the following is *not* recognized as a directory:

```
c:\folder1\subfolder2
```

If you use path macros in a path or process definition, the Bit9 Server automatically processes the macro so that it is treated as a directory, even if you don't follow the macro with a backslash. See [Using Macros](#).

## Platform-Specific Syntax

The path you provide for a rule will be interpreted according to the path rules for the platform you choose for the rule. Specifically:

- The case sensitivity of paths and file name in rules usually depends on the operating system. Rules normally are *not* case sensitive for Mac and Windows. They normally *are* case sensitive for Linux. However, if a file system with different case-sensitivity rules is attached to a system – for example by connecting an external drive or mounting a network file system – the case sensitivity of the file system determines whether a rule is effective.
- Path and file name case are preserved in the form you enter them, even for case insensitive platforms.
- Paths must use the correct directory delimiter for the rule platform: forward slash (/) for Mac and Linux and backslash (\) for Windows. Delimiters will not be converted if you change the platform for a rule, and you cannot enter the incorrect delimiter in a rule.
- Paths must meet other requirements of the chosen platform, including not using characters that are illegal in that file system (e.g., no colons (:)) in Mac paths) and not exceeding length limits.
- Any macros used in a path must be specific to the rule platform. Currently macros are limited to the Windows platform.

## Using Wildcards

You can use wildcard characters in the Path and Process fields. Asterisk (\*) indicates zero or more characters and question mark (?) indicates one character. You can use wildcards to specify partial paths or multiple paths for directories that appear in different locations on different computers (although macros might be a more effective way to accomplish this – see [Using Macros](#)). Wildcards are not allowed inside of macros.

The number of wildcards in a path or process specification is not restricted. For example, you could define a path as:

```
*\Win*\folder?\
```

### Caution

When you use wildcards, be careful not to create a rule that is so broad that it will interfere with activity in a directory that is required for legitimate use by another application or the operating system. Don't use the asterisk wildcard by itself in the path field, especially with rules that block all executions or writes, unless you are certain it will not interfere with necessary operations on agent computers. Use similar caution with wildcards when creating exceptions to restrictions created by other rules.

## Automatic Path Conversions

When a rule is processed, file paths in a process field undergo several automatic path conversions if they contain certain symbols:

- Any path that ends with a backslash (Windows) or forward slash (Mac and Linux) has the '\*' wildcard added at the end of the path.
- Any path that has no slash or drive letter has "\*" (for Windows) or "/" (for Mac and Linux) added at the beginning of the path.
- In Windows rules, drive letters may be used in a path as long as they are for local fixed volumes. Mapped drive letters should not be used because there is no guarantee that the mapping exists on all computers.
- In Windows rules, the string ".\*:" applies to all attached storage volumes except for floppy disks and CD-ROMs.

## Specifying Devices in Paths in Windows Rules

In Windows rules, you can create rules that apply to processes on some or all devices on the agent computer by including `\device\` in the path. For example:

`\device*\` specifies all devices.

`\device\harddisk*\` specifies attached storage volumes except for floppy disks and CD-ROMs.

`\device\cdrom*\` specifies CD-ROM devices.

**Platform Note:** In this release, device visibility and control features are available only for Windows computers.

## Using Macros

On the Windows platform, custom rules support certain macros in the Path and Process fields. You can see a menu of macros by typing the left angle bracket (<) character in either of these fields. There are two types of macro supported in Custom Rules:

- **Path macros** – These are a subset of the well known folders for each platform. They always identify a location rather than a specific file.
- **Registry macros** – These are macros that specify strings in the Windows Registry.



Macros can be an effective way to define a rule that works on all computers for the specified platform even when the files you want to affect are in different locations on different computers. The console displays an error message if you enter an invalid macro.

### Notes

A *path* macro can be used only at the beginning of a *Path or File* in a rule (i.e., with no other text before it in the string). A *registry* macro can be used anywhere in the Path or File specification for a Windows rule.

In this release, macros are not available for Mac and Linux rules.

## Path Macros

Path macros are based on a subset of the well-known folders for a platform (CSIDLs for pre-Vista Windows versions and KNOWNFOLDERIDs for Vista and later). Each path macro consists of a unique string surrounded by angle brackets. For example, the macro `<MyDocuments>` in a Windows rule identifies the My Documents folder for each user on each Windows computer, regardless of its actual location on an individual computer. Use the following links for further descriptions of CSIDLs and KNOWNFOLDERIDs:

[http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx)

[http://msdn.microsoft.com/en-us/library/windows/desktop/dd378457\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd378457(v=vs.85).aspx)

Because a path macro always represents a directory, it is processed as if it is followed by the directory delimiter (slash or backslash), even if you have not added one. For example, `<AppData>` in a Windows rule is interpreted as “`<AppData>`” before it is expanded, and it applies to the Application Data directory and all of its files, subdirectories, sub-subdirectories, etc. Similarly, `<AppData>myapp\` is interpreted as “`<AppData>myapp\`”. If you add a backslash yourself, the rule processor does not add a second one.

To see the menu of macros, type a left angle bracket (`<`) as the first character in the Path or File box or the Process box on the add rule page. As you type, the auto-complete menu adjusts to show only those choices matching the string you have typed so far for the platform you have chosen. [Table 50](#) shows the available path macros for Windows rules.

Notice that the table includes a “Per User” column to indicate which macros are expanded based upon the logged in user. There is a brief delay after a user is logged in before rules tied to that user will be in effect, and this delay varies depending on how many rules you have and how long it takes to expand macros or group membership in them. Because of this, rules with user-specific macros or that specify a user-group may not take effect immediately after a user logs on.

### Important

If you need a rule to be effective as soon as possible after a user logs on, do not use any of the “Per User” macros shown in the table, and do not specify a user *group* in the rule. Rules that specify a *username or SID* are always active and won't be affected by this delay.



**Table 50:** Windows Path Macros in Rules

Macro	Per User	Description
<AppData>	Yes	Directory that serves as a common repository for application-specific data. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_APPDATA</li> <li>• FOLDERID_RoamingAppData</li> </ul>
<CommonAppData>	No	Directory that contains application data used by and accessible to <i>all</i> users. This folder is used for application data that is not user specific. For example, an application can store a spell-check dictionary, a database of clip art, or a log file here. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COMMON_APPDATA</li> <li>• FOLDERID_ProgramData</li> </ul>
<CommonDesktopDirectory>	No	Directory that contains files and folders that appear on the desktop for all users. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COMMON_DESKTOPDIRECTORY</li> <li>• FOLDERID_PublicDesktop</li> </ul>
<CommonDocuments>	No	Directory that contains documents that are common to all users. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COMMON_DOCUMENTS</li> <li>• FOLDERID_PublicDocuments</li> </ul>
<CommonPrograms>	No	Directory that contains the directories for the common program groups that appear on the Start menu for all users. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COMMON_PROGRAMS</li> <li>• FOLDERID_CommonPrograms</li> </ul>
<CommonStartMenu>	No	Directory that contains the programs and folders that appear on the Start menu for all users. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COMMON_STARTMENU</li> <li>• FOLDERID_CommonStartMenu</li> </ul>
<CommonStartup>	No	Directory that contains the programs that appear in the Startup folder for all users. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COMMON_STARTUP</li> <li>• FOLDERID_CommonStartup</li> </ul>
<Cookies>	Yes	Directory that serves as a common repository for Internet cookies. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_COOKIES</li> <li>• FOLDERID_Cookies</li> </ul>
<DesktopDirectory>	Yes	Directory used to physically store file objects on the desktop (not the desktop folder itself). <ul style="list-style-type: none"> <li>• CSIDL_DESKTOPDIRECTORY</li> <li>• FOLDERID_Desktop</li> </ul>

Macro	Per User	Description
<InternetCache>	Yes	Directory that serves as a common repository for temporary Internet files. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_INTERNET_CACHE</li> <li>• FOLDERID_InternetCache</li> </ul>
<LocalAppData>	Yes	Directory that serves as a data repository for local (non-roaming) applications. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_LOCAL_APPDATA</li> <li>• FOLDERID_LocalAppData</li> </ul>
<MyDocuments>	Yes	Virtual folder that represents the My Documents folder. The file system directory used to physically store a user's common repository of documents. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PERSONAL</li> <li>• FOLDERID_Documents</li> </ul>
<Profile>	Yes	User's profile folder. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PROFILE</li> <li>• FOLDERID_Profile</li> </ul>
<ProgramFiles>	No	Program Files folder. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PROGRAM_FILES</li> <li>• FOLDERID_ProgramFiles</li> </ul>
<ProgramFilesx86>	No	32-bit Program Files folder. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PROGRAM_FILESX86</li> <li>• FOLDERID_ProgramFilesX86</li> </ul>
<ProgramFilesCommon>	No	Folder for components shared across applications. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PROGRAM_FILES_COMMON</li> <li>• FOLDERID_ProgramFilesCommon</li> </ul>
<ProgramFilesCommonx86>	No	32-bit Program Files folder. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PROGRAM_FILES_COMMONX86</li> <li>• FOLDERID_ProgramFilesCommonX86</li> </ul>
<Programs>	Yes	Directory that contains the user's program groups (which are themselves file system directories). Maps to: <ul style="list-style-type: none"> <li>• CSIDL_PROGRAMS</li> <li>• FOLDERID_Programs</li> </ul>
<RecycleBin>	Yes	Directory for the Recycle Bin. The location depends on the type of operating system and file system. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_BITBUCKET</li> <li>• FOLDERID_RecycleBinFolder</li> </ul>
<StartMenu>	Yes	Directory that contains Start menu items. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_STARTMENU</li> <li>• FOLDERID_StartMenu</li> </ul>

Macro	Per User	Description
<Startup>	Yes	Directory that corresponds to the user's Startup program group. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_STARTUP</li> <li>• FOLDERID_Startup</li> </ul>
<System>	No	The platform-specific Windows System folder. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_SYSTEM</li> <li>• FOLDERID_System</li> </ul>
<Systemx86>	No	32-bit "System" folder on both 32-bit and 64-bit operating systems. Allows you to specify that a rule applies only to 32-bit versions of utilities. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_SYSTEMX86</li> <li>• FOLDERID_SystemX86</li> </ul>
<Windows>	No	The Windows directory or SYSROOT. This corresponds to the %windir% or %SYSTEMROOT% environment variables. Maps to: <ul style="list-style-type: none"> <li>• CSIDL_WINDOWS</li> <li>• FOLDERID_Windows</li> </ul>

## Windows Registry Macros

For Windows rules, Registry (Reg) macros provide access to Windows Registry values, which you can use in a Path or Process specification. Unlike path macros, reg macros have variable content between their brackets. A Reg macro must resolve to a value, not a key.

### To enter a Reg macro:

1. Begin by typing a left angle bracket (<) followed immediately by **Reg**:
2. Follow <Reg: with one of the following:
  - a. **HKLM\** (or HKEY\_LOCAL\_MACHINE)
  - b. **HKCU\** (or HKEY\_CURRENT\_USER)
  - c. **HKLM-SoftwareX86\**
  - d. **HKLM-SoftwareX64\**
  - e. **HKCU-SoftwareX86\**
  - f. **HKCU-SoftwareX64\**
3. Enter the rest of the path you want in this rule. This should specify a value, not a key, with one exception – you can provide a key specification and follow it by a backslash to use the default value for this key.
4. Because reg macros contain variable content, they do not auto-complete. You must provide the whole path you want in the macro and end the macro with the right angle bracket (>). The resulting macro will have a format like the following (using HKLM as the top-level Registry node example here):

```
<Reg:HKLM\YourSpecifiedPath>
```

Reg macros are evaluated on each agent the first time the rule becomes available to that agent. If the rule is valid for that computer, it is enabled. For example, it is possible to create a rule that Promotes an updater for an application called “MyApp” by using the path value written to the registry. On systems with MyApp Update installed, <Reg:HKLM\Software\MyApp\Update\path> might expand to C:\Program Files (x86)\MyApp\Update\ MyAppUpdate.exe. On systems that did not include the update program, the rule would not be created.

Once evaluated, rules that use Reg macros are not re-evaluated on a computer unless certain conditions occur. This means that changes to the Registry during a session might not affect rule behavior, even if the change would enable or disable the rule. The conditions that cause "re-expansion" of rules on an agent are:

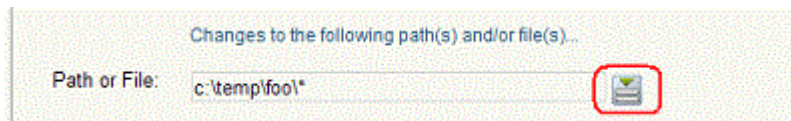
- the agent is stopped and restarted (e.g., by shutting down and restarting the computer)
- a new user logs in
- the agent is reassigned to a policy with different rules
- rules are created, edited or deleted on the server
- the agent detects the end of an MSI install/upgrade
- manual re-evaluation is triggered using a special Bit9 Support command.

### Important

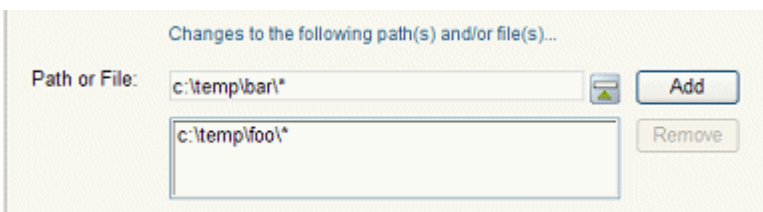
If you specify an HKCU-based registry macro in a rule, that rule won't become active for a particular user until a short time after the user is logged on. The amount of time can vary depending upon how many rules you have and how long it takes to expand registry macros and other user-based parameters. Avoid using the HKCU macro if you need a rule to be effective immediately after login.

## Entering Multiple Paths or Processes

For both the Path or File value and the Process value in a rule, you can enter more than one string. When you have entered the first Process for this rule, click the Expand button to the right of the box.



You can then add additional paths or files by typing them in the box and clicking **Add** after each one.



You can remove any file or path by selecting the file or path in the list below the Path or File box, and clicking the **Remove** button.

If you enter multiple paths or processes for a rule, the Custom Rules page shows the first path and then **(multiple)** in the relevant column for this rule. Moving the mouse over the value shows a tooltip with the complete list of paths or processes for the rule.

## Specifying Processes

You can specify the Process string using the same options available for Path or File. See [“Specifying Paths and Processes”](#) on page 345 for complete details.

If you specify both a User or Group and a Process for a rule, they work together. For example, if you choose Specific Process, a matching user or group must be running a matching process for the rule to be applied. If you choose Any Process Except, the rule is applied unless *both* the User or Group and the Process match the rule definition.

**Table 51:** Process Menu Choices

Menu Choice	Description
<b>Any Process</b>	Apply the rule no matter what process attempts to execute or write files matching the rule.
<b>Any Promoted Process</b>	Apply the rule when a process that is <i>promoted</i> at the time the rule is evaluated attempts an action matching the rule. A promoted process is any approved process that is generated by a file marked as an installer, or has been promoted as a consequence of a custom rule, or is an approved process launched by a promoted process.
<b>Any System Process</b>	Apply the rule when a process that is running under the security context of the Local System user attempts an action matching the rule. This choice has the same effect as choosing Local System in the User or Group menu, but may be more efficient.
<b>Specific Process...</b>	Apply the rule when a process matching a string you specify attempts an action matching the rule. You can enter one or more processes in the text box below the menu.
<b>Any Process Except...</b>	Apply the rule when any process <i>except</i> one matching a string you specify attempts an action matching the rule. You can enter one or more processes in the text box below the menu.

## Specifying Users or Groups

For certain rule types, you can create a rule that applies only when specific users or users in specific groups attempt an action. The choices for User or Group on the Add/Edit Custom Rule page are:

- **Any Users** – applies the rule to all users.
- **Specific User or Group...** – opens a text box below the menu, in which you can enter AD users or groups in the format *userorgroupname@domain* or *domain\userorgroupname*  
**Platform Note:** To specify a Mac or Linux group, you must precede it with the word “group” and a colon. For example, you would enter *group:consoleusers* for the “consoleusers” group. Without the prefix, group names will be considered user names.
- For Windows rules only, there are other menu choices that are built-in Windows groups, such as **Authenticated Users** and **Local Administrators**.

### Notes

- When running on Windows Vista and later, membership in pre-defined security groups like Administrators requires that the application run as an administrator. If a group definition is necessary for a rule, consider using security groups you have defined rather than the pre-defined groups
- There is a brief delay after a user logs in before group membership is established and group-based rules become effective. This delay may be longer if you have a large number of rules. If a rule must be effective as soon as possible after a user logs on, do not specify a user *group* in the rule. Rules that specify a *username* or *SID* are always active and won't be affected by this delay.
- Specifying a user or group also determines whether macros in a path are expanded. Only paths whose macros match the specified user or group are expanded, and so even if the user or group is attempting the action, if the path includes a user-related macro, paths that would evaluate to a user other than those specified are not expanded and the rule is not effective.

## Rule Ranking

Custom rules have a “Rank” number and are evaluated from lowest number to highest number, beginning with the rule ranked ‘1’. By default, rules appear in their rank order, but you can re-sort the table by other columns if you choose. If a file matches one rule that blocks an action and another rule that allows it, the highest ranking rule (that is, the one with the lowest number), takes precedence and the lower-ranked (higher number) rule has no effect. You can change the ranking of rules if you decide that you want one of your rules to be considered before its current position.

### Important

Rule ranking is significant only for rules that Block, Allow, or Prompt the user to block or allow. The highest ranking block, allow, or prompt rule that matches an attempted file action not only takes precedence but stops processing of any lower-ranked rules matching the action.

A rule whose action is Approve, Approve as Installer, Track, Report, Promote or Ignore does not stop processing of lower-ranked rules. For example, if a write attempt first matches an Ignore rule and also matches another rule with a lower rank (higher number) on the list, the second rule will also be processed.

Although not custom rules, *Internal* rules for fundamental actions in the Bit9 Security Platform, such as blocking banned files, are included in the Custom Rules table. See [“Rule Ranking and Internal Rules”](#) for suggestions about how and when you might change the order of other rules relative to internal rules.

**To change the rank of a custom rule:**

1. On the Custom Rules page, if the rules are not currently sorted by rank, click on the Rank column head to sort them.
2. Find the rule whose rank you want to change.
3. To give the rule a higher rank, click the up arrow button next to the rule until it is ranked appropriately.

**-or-**

Move the mouse cursor over the rule you want to move, hold down the left mouse button, drag the rule to the new location, and release the mouse button.

4. To give the rule a lower rank, click the down arrow next to the rule until it is ranked appropriately, or use the drag-and drop method to move the rule.

Rank ▲	Rule Type	Name	Action
1	Execution Control	[Sample] Visual Studio 2010 Promote Build	Allow and Promote executes
2	Advanced	[Sample] Microsoft App-V Interoperability	Allow executes, Ignore writes
3	Execution Control	Allow .NET dll executions	Allow executes
4	Performance Optimization	Ignore Recycle Bin	Ignore writes
5	Performance Optimization	Ignore System Restore	Ignore writes
6	Performance Optimization	Ignore Outlook Files	Ignore writes
7	Performance Optimization	Ignore Data Files	Ignore writes

**Note**

When using drag-and-drop, you cannot drag rules between pages. If you need to move a rule to a ranking not currently shown, you can increase the number of rows shown per page by using the menu at the bottom right corner of the Custom Rules page.



## Rule Ranking and Internal Rules

The Custom Rules table includes Internal rules related to features presented in other parts of the console. These built-in rules are approximately equivalent to the settings you see when you view the Device and Advanced Settings on the Edit Policy page.

The image shows two screenshots from the Bit9 console. The top screenshot is titled "Device Control Settings for Standard Protection" and lists six rules with their status and notifier settings. The bottom screenshot is titled "Advanced Settings for Standard Protection" and lists twelve rules, including "Block banned file hashes" which is highlighted in the text.

Name	Status	Notifiers
Block writes to unapproved removable devices	Off	<default>: Block writes to unapproved removabl
Block writes to banned removable devices	Active	<default>: Block writes to banned removable de
Report reads from unapproved removable devices	Off	<none>
Report reads from banned removable devices	Off	<none>
Block executions from unapproved removable devices	Off	<default>: Block executions from unapproved re
Block executions from banned removable devices	Active	<default>: Block executions from banned remov

Name	Status	Notifiers
Block unanalyzed scripts and executables	Active	<default>: Block unanalyzed scripts and execu
Block unapproved scripts	Active	<default>: Block unapproved scripts
Block unapproved executables	Active	<default>: Block unapproved executables
Block banned file names	Active	<default>: Block banned file names
Block banned file hashes	Active	<default>: Block banned file hashes
Block executables run from a network drive	Off	<default>: Block executables run from a networ
Block files with banned publishers or certificates	Active	<default>: Block files with banned publishers or
Enforce memory rules	Active	<default>: Enforce memory rules
Enforce registry rules	Active	<default>: Enforce registry rules
Enforce custom (file and path) rules	Active	<default>: Enforce custom (file and path) rules
Enforce tamper protection	Active	<default>: Enforce tamper protection
Terminate processes with banned images	Report Only	<default>: Terminate processes with banned im

For example, *Block banned file hashes* is listed as an Internal Rule on the Custom Rules page and as a setting in the Advanced Settings section of the Edit Policy page.

		34	Disabled	Windows	Advanced	[Sample] Tamper Protection	Allow writes
		35	Disabled	Windows	Advanced	[Sample] Tamper Protection	Block writes
		36	Enabled	Mac	Advanced	MDS	Silence writes
		37	Disabled	All Platforms	Internal	Block executables run from a network drive	Block executes
		38	Enabled	All Platforms	Internal	Block executions from banned removable devices	Block executes
		39	Disabled	All Platforms	Internal	Block executions from unapproved removable devices	Block executes
		40	Enabled	All Platforms	Internal	Block writes to banned removable devices	Block (Hidden) writes
		41	Disabled	All Platforms	Internal	Block writes to unapproved removable devices	Block (Hidden) writes
		42	Enabled	All Platforms	Internal	Block files with banned publishers or certificates	Block executes
		43	Enabled	All Platforms	Internal	Block banned file hashes	Block executes
		44	Enabled	All Platforms	Internal	Promote processes from trusted users	Promote executes

You cannot enable, disable, modify or move Internal rules in the Custom Rules table – their delete and edit buttons are greyed out and they do not have up or down arrows. The order of Internal rules cannot be changed relative to each other. However, you can change the rank of any Internal rule relative to other, non-internal Custom Rules to better control how and when different rules are enforced. You do this by moving the other rule (not the Internal rule).



The following are key situations in which you might want to change the order of Internal rules relative to other rules.

- By default, if a file has been banned but you create a Custom Rule specifying that the file is allowed to execute, that rule appears higher in rank than the internal rule that blocks executions of banned hashes. Because of this, the custom rule takes precedence over a hash ban on that file. However, if you move the Custom Rule that allows the banned file to execute to a rank below the Internal rule *Block banned file hashes*, the file will *not* be allowed to execute.
- By default, if you create a Custom Rule that allows a file to be written, it appears higher in rank than internal rules that block writing, and so the allow rule takes precedence. For example, you might create a rule that allows writes to a device, and that will appear above the internal rule that blocks writes to a device. However, if you move the Custom Rule that allows device writes to a position below the *Block writes to unapproved removable devices* rule, the block rule takes precedence and a file on an unapproved device is blocked from writing, even if it matches an Allow or Prompt rule below.

#### To make file hash bans take precedence over custom rules that allow execution:

1. On the Custom Rules page, if the rules are not currently sorted by rank, click on the Rank column head to sort them.
2. Find the rule that allows execution of the banned file.
3. Use the down arrow to move the allow rule to a position below the *Block banned file hashes* rule.



The screenshot shows a table of custom rules. Rule 31, 'Allow Mystery App to Execute', is highlighted with a red box and is positioned below rule 30, 'Block banned file hashes'. This visualizes the step of moving the allow rule below the block rule to ensure the block rule takes precedence.

29	Internal	Block files with banned publishers or certificates	Block executes
30	Internal	Block banned file hashes	Block executes
31	Execution Control	Allow Mystery App to Execute	Allow executes
32	Internal	Promote processes from trusted users	Promote executes
33	Internal	Block unapproved executables	Block executes

## Disabling or Deleting Custom Rules

If you do not want a custom rule to be effective anymore, you can either disable it, which leaves it in the custom rules table, or delete it from the table. In either case, the rule stops affecting newly discovered files. However, files that were affected by the rule before it was disabled retain any file state assigned to them by the rule.

If you think you might use the rule again, disabling it temporarily is the best choice.

#### To disable a custom rule:

1. In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Custom** tab. The Custom Rules table appears.
2. Click the Edit button (pencil and file) next to the rule you want to disable. The Edit Custom Rule page appears.
3. In the Status line, click the **Disabled** radio button, and then click the **Save** button at the bottom of the page. The rule is now disabled.

Deleting a rule eliminates it permanently – there is no undo or retrieval for a deleted rule. Because of that, be sure you actually want to delete the rule. Deletion of the rules that were pre-configured in the Bit9 Console is not recommended.

**To delete a custom rule:**

1. In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Custom** tab. The Custom Rules table appears.
2. Click the Delete button (red circle with X) next to the rule you want to delete, and click **OK** on the configuration dialog. The rule is now deleted.

## Viewing Rule Status on Computers

Depending upon the number of agents managed by your Bit9 Server and the number that are disconnected, not all agents might receive new or updated rules in a short amount of time. The Related Views menu on the Edit page for an enabled rule provides links to two different filtered views of the Computers page to help determine the status of the rule on agent-managed computers. The choices are:

- **All Computers that have received this rule**
- **All Computers that have not yet received this rule**

This menu does not appear for rules that have never been enabled.

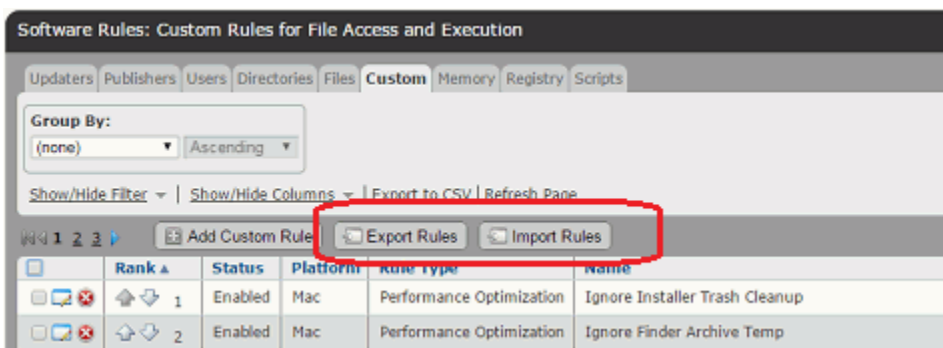
## Exporting and Importing Rules

Certain rules created on one Bit9 Server may be exported to a file and then imported from the file to another Bit9 Server. The following rule types are exportable:

- Custom Rules
- Registry Rules
- Memory Rules

Rule export and import can be useful in several different situations:

- **Transfer from Test to Production Environments** - You may want to create, test and perfect rules in a lab environment before you apply them to your production server. With rule export and import, once you are satisfied with rule behavior, you can export rules from the test server and import the rule file to the production server, eliminating the effort and error potential of manual re-entry of the rule parameters.
- **Rule Sharing in the Bit9 Community** - Users who have created a rule or set of rules they consider particularly useful can make their rule(s) available in a file that may be imported by other members of the community.
- **Solutions from Bit9 Support** - If you need assistance in creating a rule to accomplish a particular outcome, Bit9 Support may be able to provide an appropriate rule and you will be able to import it to your server.



You export and import of rules on the Software Rules page tab that shows the rule table for each of the exportable rule types. One or more rules of the same type may be included in an export file, but rule types are not mixed in the same file; for example, you cannot mix custom and registry rules in the same file.

Exported rule files are downloaded using the standard download mechanism and target location for the browser in which the console is displayed. They have the extension **.rules**. As new rules are created or existing rules changed, new export files may be generated as needed.

Rule files are encrypted to prevent tampering. When a file is exported, it can be further protected with an optional password.

### Note

Rules may be exported and imported only from and to Bit9 Servers at version 7.2.1 and later.

## Exporting Rules

When exporting rules, consider the destination of the rules. You might export one set of rules for internal use and another to share with other members of the Bit9 community. The following are some points to keep in mind when exporting rules:

- **Proprietary Information** – It is possible that a rule could reveal information that you would prefer not to share outside your organization. This might include path or user names, or comments in the Description field of a rule. Note that you can choose not to export user and group specifications that are not well known SIDs.
- **Environment Dependencies** – For rules shared outside your environment, hard paths could limit the usefulness of a rule. Rules using macros might be more portable.

### To export rules to a file:

1. In the console menu, choose **Rules > Software Rules** and click on the tab for the type of rules (Custom, Registry, or Memory) you want to export.
2. All of the rules you want to export to one file must be on the current page. If necessary, use filters, grouping, or a Saved View to change the page content. If you are exporting a large number of rules, you might also need to change the number of rows shown per page with the control in the bottom right corner of the console page.
3. Check the box next to each rule you want to export and then click the **Export Rules** button.



The Export Rules dialog appears. It shows the number of rules to be exported, provides a field in which to name the file, and includes other export options.

4. Enter the file name (without extension) for the new Export File. This is the only mandatory field.

The screenshot shows a dialog box titled "Export Rules" with a close button in the top right corner. Below the title, it says "Number of rules for export: 4". There are four main input sections:
 

- Export File Name:** A text input field containing "ABC and EXEmaker Rules" and a ".rules" button to its right.
- Password (Optional):** A text input field with the placeholder text "Enter password to encrypt export file."
- Confirm Password:** A text input field with the placeholder text "Enter password to confirm."
- Export SIDs:** A checkbox that is currently unchecked.
- Description:** A larger text area containing the text "Rules to allow execution and ignore temp file writes for two new company apps."

 At the bottom of the dialog are two buttons: "Export" and "Cancel".

5. Exported rules files are not readable as text, but if you would like to further protect the file, enter and confirm a password. Be sure to have the password available for the users who will be importing the file.
6. Check the **Export SIDs** box if all of the following is true:
  - One or more of the rules you are exporting specify that they should be applied only for specific users or groups.
  - These users or groups are *not* one of the well-known security identifiers (SIDs) on Windows systems.
  - You are planning to import these rules to a server on which your non-well-known SIDs will be present. This is more likely to be the case if you are transferring rules within the same organization.
7. If you choose, add a Description that will help anyone importing rules from this file better understand what their purpose is.
8. When you are ready to save the Export File, click the **Export** button. The dialog closes and the rules file is created using the standard download mechanism of the browser running the Bit9 Console. For example, if you entered “New Custom Rules” in the Export File Name field, a file named “New Custom Rules.rules” might be written to the Downloads folder.

Once you have exported rules to a file, you can copy it to the host of another Bit9 Server or make it available via a network connection for import.

## Importing Rules

When you want to import rules from another server, you need access to a rules file. In addition, if the file was passworded, you need the password to open it in the import dialog and choose the rules to import.

The steps for importing rules are shown in [“To import rules from a file:”](#) on page 365. Before doing an import, it is highly recommended that you read the following sections.

## Selecting Rules to Import

When you enter the name of a rules file in the Import Rules dialog, the file is checked to determine whether it is properly formed and also to be sure that the rule type matches the page on which the import is being attempted. If it is passworded, you are prompted to enter the password. Assuming it passes these checks, the rules it contains are listed in the dialog box.

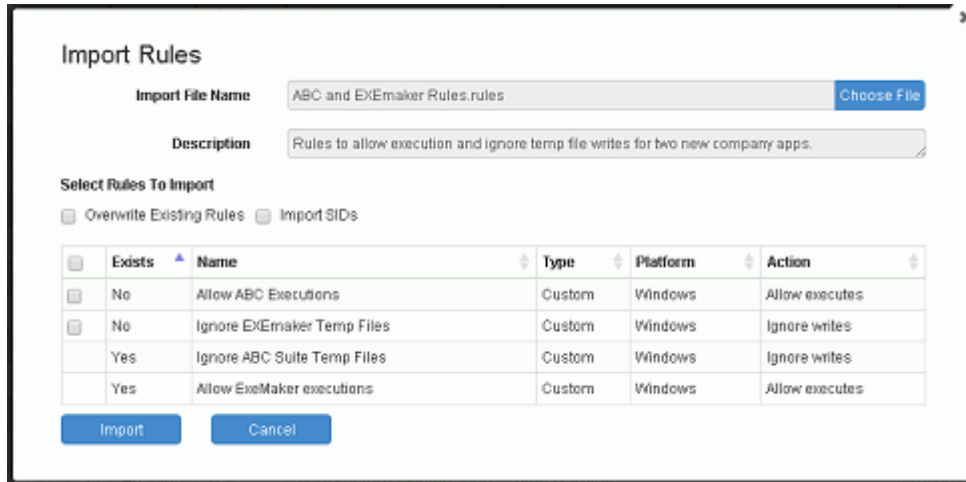


Table 52 describes the fields on the Import Rules dialog, most of which are described in more detail later in this section.

**Table 52:** Import Rules Dialog Fields

Field	Description
<b>Import File Name</b>	Shows the name of the file from which rules will be imported to this server. File names are entered using the Choose File button and file chooser dialog.
<b>Description</b>	Shows the description provided when the rules were exported, if any.
<b>Overwrite Existing Rules</b>	If not checked (the default), there is no checkbox next to rules that already exist on the target server. If checked, all rules in the table have checkboxes, and you may choose to overwrite an existing rule.
<b>Import SIDs</b>	If not checked, user and group specifications in rules are not imported if those users or groups are not well-known Security IDs (SIDs), such as Local Administrator. If checked, all user and group specifications in rules are imported. Note that there is a matching option for exporting rules, and so some rules in an exported file might not include user and group specifications that are in the original rule.
<b>Enter Password</b>	Appears only if a password was specified during rule export. If present, shows a field in which to enter the password to open this file and an Open Import File with Password button.

Field	Description
<b>Rules Table</b>	<p>All rules included in the import file are listed in a table. The row for each rule includes the following columns:</p> <ul style="list-style-type: none"> <li>• (Checkbox) – A checkbox appears next to each rule that can be selected for import.</li> <li>• Exists – Indicates whether the rule already exists on the target server.</li> <li>• Name – The name of the rule as it appears on the rules page.</li> <li>• Type – The type of rule as indicated by the tab on which it appears (Custom, Memory, or Registry).</li> <li>• Platform – The operating system/platform to which the rule applies (Windows, Mac, Linux).</li> <li>• Action – The action type taken by the rule.</li> </ul>

Each rule on a Bit9 Server has a globally unique identifier (GUID), and that ID is included when it is exported to a file. When a rules file is chosen for import, the GUIDs of the incoming rules are compared to the GUIDs of existing rules, and if a rule already exists on the server, that fact is shown on the Import Rules dialog.

Depending upon the source of the rules (internal to your organization, the Bit9 community, Bit9 Support), you might make different decisions about which rules to import. You do not have to import all rules in a file. A checkbox next to each available rule allows you to choose which rules to import.

By default, any rules in the import file that already exist on the server do not have a checkbox next to them. However, there is a master checkbox named Overwrite Existing Rules that activates checkboxes for these rules, allowing you to import any rule (including existing rules) listed on the page.

**Import Rules**

Import File Name: ABC and EXEmaker Rules.rules Choose File

Description: Rules to allow execution and ignore temp file writes for two new company apps.

Select Rules To Import

Overwrite Existing Rules  Import SIDs

Exists	Name	Type	Platform	Action
<input type="checkbox"/>	Allow ABC Executions	Custom	Windows	Allow executes
<input type="checkbox"/>	Ignore EXEmaker Temp Files	Custom	Windows	Ignore writes
<input type="checkbox"/>	Ignore ABC Suite Temp Files	Custom	Windows	Ignore writes
<input type="checkbox"/>	Allow EXEmaker executions	Custom	Windows	Allow executes

Import Cancel

## Differences in Settings for Imported Rules

Rules contain a variety of parameter types, including processes and paths, actions to take, and notifiers to use if a block is involved. Most of the settings for an imported rule remain the same as they were on the server from which they were exported, but there are some variations depending on the following factors:

- Whether an imported rule is *new or updates an existing rule* on the target server
- Whether the rule specifies that it applies only to *certain policies*
- Whether the rule specifies that it applies to *certain users or groups*

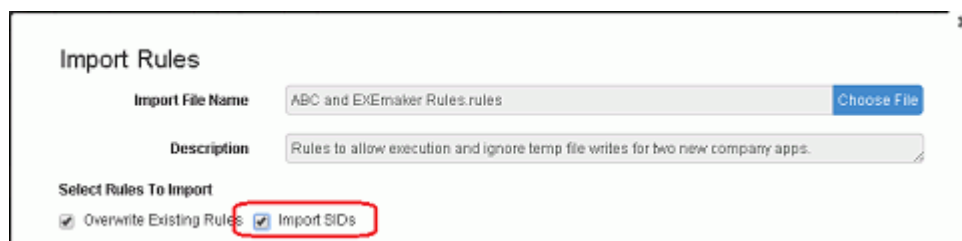
The following setting differences depend upon whether a rule is new or already existed on the server:

- **Enabled or Disabled** – New rules are disabled when imported and must be enabled to take effect. This gives you the ability to customize a rule, including providing any site-specific policy or user parameters, before enabling it. When existing rules are overwritten by an import, the enable/disable settings on the target server are kept.
- **Rank** – New rules are ranked at the highest level when imported. Existing rules that are overwritten by an import maintain their previous relative rank on the target server (moving down in rank accordingly if new rules were also part of the import)
- **Notifier** – If a new imported rule requires a notifier (i.e., if it blocks an action), the default notifier is used. If an imported rule overwrites an existing rule, the notifier specified in the existing rule will be kept.

Some rules are specified to apply only to computers in certain policies. However, policies on one server may not exist on another. If an imported rule is new, any previous policy specification is removed and the rule applies to all policies. If an imported rule overwrites an existing rule, the policy setting in the existing rule on the target server is maintained – any policy specification in the rule from the exporting server is not applied.

Some rules are specified to apply only if certain users or members of certain groups are taking an action. There are user and group names that are well known Security Identifiers (SIDs) that can be expected to be available on all Windows computers. However, users and groups that are not well known might not exist on computers to which rules are imported. If an exported rule specifies users or groups, the results of an import depend on whether the user or group is well known and on whether several things:

- All well-know SIDs will always be exported and imported in a rule specification.
- If the Export SIDs checkbox was checked on the Export Rules dialog when the rules were exported, specifications for users and group that are not well-known will also be exported with their rules.
- If the Import SIDs checkbox is checked on the Import Rules dialog, specifications for users and group that are not well-known will also be imported, *if they were exported with the rules*.



- If a both well-known and non-well-known SIDs are specified in an exported rule and the Import SIDs checkbox is not checked, the rule is exported with the well-known users or groups only. If the rule only specifies users or groups that are not well known, the user or group specification is removed from the rule and it applies to all users.



**To import rules from a file:**

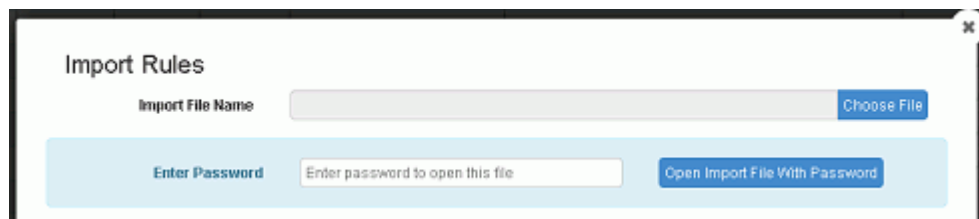
1. In the console menu, choose **Rules > Software Rules** and click on the tab for the type of rules (Custom, Registry, or Memory) you want to import.

2. Click the **Import Rules** button.

The Import Rules dialog appears.

3. Click the **Choose File** button to open a standard Windows file chooser dialog and choose the file whose rules you want to import.  
If no password is required, the Import Rules dialog show a table of the available rules, as shown in [“Selecting Rules to Import”](#) on page 362.

4. If the file requires a password, the dialog shows fields for password entry before displaying any rule names. In this case, enter the password and click Open Import File With Password.



When the password is verified the dialog shows the table of available rules, as shown in [“Selecting Rules to Import”](#) on page 362.

5. If you want to include any user or group parameters that do are not well-known SIDs, check the **Import SIDs** box. See [“Selecting Rules to Import”](#) on page 362 for an explanation of these feature.

6. By default, there is no checkbox for any rule that is already present on the target server. If you want the option of choosing to overwrite one or more existing rules, check the **Overwrite Existing Rules** box. See [“Differences in Settings for Imported Rules”](#) on page 363 for what happens when you overwrite an existing rule.

7. In the dialog, examine the information about each rule, check the box next to each rule you want to import, and then click the **Import** button.

The dialog closes and the rules are imported to the server. Rules that have been imported appear in bold italic on the rules page for the duration of the current session.

	Rank ▲	Status	Platform	Rule Type	Name	Action
<input type="checkbox"/>	1	Disabled	Windows	Performance Optimization	<i>Ignore EXEmaker Temp Files</i>	Ignore writes
<input type="checkbox"/>	2	Disabled	Windows	Execution Control	<i>Allow ABC Executions</i>	Allow executes
<input type="checkbox"/>	3	Disabled	Windows	Execution Control	<i>Allow ExeMaker executions</i>	Allow executes
<input type="checkbox"/>	4	Disabled	Windows	Performance Optimization	<i>Ignore ABC Suite Temp Files</i>	Ignore writes
<input type="checkbox"/>	5	Enabled	Mac	Performance Optimization	Ignore Installer Trash Cleanup	Ignore writes
<input type="checkbox"/>	6	Enabled	Mac	Performance Optimization	Ignore Finder Archive Temp	Ignore writes

## Custom Rule Types and Examples

The Rule Type menu on the Add/Edit Custom Rule page provides the following options:

- **File Integrity Control** – Protects specified folders or files from being modified.
- **Trusted Path** – Defines folders or files for which file execution is always allowed.
- **Execution Control** – Controls behavior when an attempt is made to execute a file matching the rule.
- **File Creation Control** – Controls behavior when an attempt is made to write a file matching the rule.
- **Performance Optimization** – Specifies folders or files to avoid tracking (execution will still be monitored).
- **Advanced** – Provides the greatest selection of options for controlling file execution, creation, and/or tracking.

The Custom Rules table includes several rules marked as *[Sample]* – these rules are disabled by default. For example, *[Sample] Developer - Visual Studio Ignore Intermediate Files* is a Performance Optimization rule that instructs Bit9 to ignore certain intermediate files typical of many build environments. In the Custom Rules table, you can click the Edit (pencil) button next to any of these samples to examine the types of parameter choices that might be applied to accomplish similar results.

The sections below provide general examples of some of the different rule types.

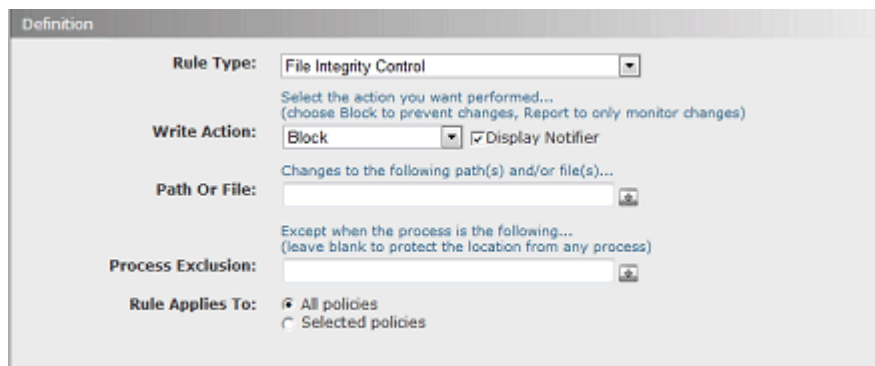
### File Integrity Control

**Write Action Options:** Block, Report

**Execute Action:** Does not apply to this rule type (not shown)

**Users:** Applies to all users (fixed value for this rule type, not shown)

File Integrity Control rules allow you to control modifications to a specific folder (or file) or folders (or files) matching your specification. You can write-protect the folder(s) by choosing Block as the Write Action, or you can monitor (but not block) changes by choosing Report as the Write Action.



The screenshot shows the 'Definition' form for a File Integrity Control rule. The 'Rule Type' is set to 'File Integrity Control'. The 'Write Action' is set to 'Block', and the 'Display Notifier' checkbox is checked. The 'Path Or File' field is empty, and the 'Process Exclusion' field is also empty. The 'Rule Applies To' section has 'All policies' selected.

For example, perhaps you use an application called ScheduleCreator to generate schedules for everyone at your company and put the results in a **Schedule** folder in the **My Documents** folder on each user's computer. Assume that the ScheduleCreator executable is called **makesched.exe**. You want to be able to generate the schedule for each user, but you want to make sure nobody can change the schedules in the designated location once

generated. You could choose **File Integrity Control** as the rule type and leave **Block** as the Write Action. Then you could enter **<MyDocuments>\Schedule\** as your Path or File. Note that **<MyDocuments>** is a macro that maps to the My Documents folder for each user on computers running the agent. Finally, in the Process Exclusion box, you could enter **\*\makesched.exe** so that this process will be allowed to write to the path in the rule. Use of a macro in the Process Exclusion box could further restrict the allowable process to one run from a specific location, such as **<ProgramFiles>\Schedule Maker\makesched.exe**.

The screenshot shows the 'Add Custom Rule' dialog box with the following configuration:

- General:**
  - Name: Block Unauthorized Writes to Schedule Folder
  - Description: Block any attempts to modify schedules in the Schedule folder unless by Schedule Maker application.
  - Status:  Enabled  Disabled
  - Platform: Windows
- Definition:**
  - Rule Type: File Integrity Control
  - Write Action: Block (Use Policy Specific Notifier is checked)
  - Path Or File: <MyDocuments>\Schedule\
  - Process Exclusion: <ProgramFiles>\Schedule Maker\makesched.e
  - Rule Applies To:  All policies  Selected policies

## Trusted Paths

**Execute Action:** Allow, Allow and Promote, Promote

**Users:** Applies to all users (fixed value for this rule type, not shown)

One use of custom rules is designation of a trusted path. You can designate a network location as a trusted path and place installers there so that computers in certain policies or all policies can execute them.

A trusted path is an access method, *not* a global approval method. It allows execution of files in a specific location without globally approving files generated by the executable.

Any files in a trusted path must be executed in the specified location; the destination of the files *resulting* from an execution can be another computer (i.e., the computer accessing the executable via a trusted path). Computers with access to files on the trusted path cannot execute an installation package by copying it to their own machine and executing it there.

Files generated by an executable in the trusted path are locally approved on the computer on which they are installed (unless there is a global or by-policy ban on the file). If the new files have not been seen by the Bit9 Server before, they are added to the File Catalog tab of the Files page with a status of Unapproved.

### Important

- Any user who is able to write executables or scripts into the trusted path can make any application available to any computer that (a) has access to that location and (b) permits executions from remote drives. Before you enable a trusted path, check the platform's security settings for that location to ensure that it is properly protected.
- In the Bit9 Console, one way to help protect a Trusted Path is to create a user-specific File Integrity Control or File Creation Control rule for the same path. If you rank the new rule higher than the Trusted Path rule, you can control writes to the path while still allowing its use as a software distribution location.

To create a trusted path for installers, follow the instructions in [“Creating a Custom Rule”](#) on page 338, choosing **Trusted Path** as the Rule Type. Note that when you choose Trusted Path, other fields on the page change to reflect your choice. The Execute Action menu shows **Allow**, meaning that files matching this rule will be allowed to execute.

The screenshot shows the 'Definition' window for a rule. The 'Rule Type' dropdown is set to 'Trusted Path'. Below it, a note says 'Select the action you want performed... (promoted processes are allowed to create approved files)'. The 'Execute Action' dropdown is set to 'Allow'. Below that, a note says 'Files when executed from the following path(s)... (specific filenames may be entered)'. The 'Path Or File' field is empty. Below that, a note says 'Only when executed by the following process(es)... (select 'Any Process' to allow execution regardless of parent process)'. The 'Process' dropdown is set to 'Any Process'. At the bottom, 'Rule Applies To' has two radio buttons: 'All policies' (which is selected) and 'Selected policies'.

For example, you might use an application called FileDistributor to distribute your company software via some distribution server. Assume that the FileDistributor application is actually an executable called **filedist.exe**, and that your company's software is deployed from a distribution server located at `\\FILE2DEPLOY\Apps\`. You could choose **Trusted Path** as the rule type and enter `\\FILES2DEPLOY\Apps\*` as your Path or File.

If you leave the Process field for this rule set to **Any Process**, any process on a client affected by the rule can run applications and installers from that location. To reduce the security gaps in your custom rule, you might want to limit the right to execute files in this directory to FileDistributor itself, such that *only* FileDistributor can install applications from the named directory. By making the Process `*\filedist.exe`, you create just such a restriction. You can be even more specific by using a macro to identify the file location; for example, `<ProgramFiles>\FileDistributor\filedist.exe`. A user *manually* trying to run those same files will be blocked.

**Add Custom Rule**

**General**

**Name:** Allow File Distribution from Deployment Folder

**Description:** Allow executions in standard file deployment directory by the file distribution application

**Status:**  Enabled  Disabled

**Platform:** Windows

---

**Definition**

**Rule Type:** Trusted Path

Select the action you want performed...  
(promoted processes are allowed to create approved files)

**Execute Action:** Allow

Files when executed from the following path(s)...  
(specific filenames may be entered)

**Path Or File:** WFILES2DEPLOYApps!

Only when executed by the following process(es)...  
(select 'Any Process' to allow execution regardless of parent process)

**Process:** Specific Process...  
<ProgramFiles>FileDistributorfiledist.exe

**Rule Applies To:**  All policies  
 Selected policies

You can further limit trusted paths and any other custom rules to computers in one or more specific policies, using the “Rule applies to” buttons. By combining all of these parameters, you have the opportunity to define a rule that allows you to accomplish necessary operations while exposing your systems to as little security risk as you can.

## Execution Control

**Execute Action Options** – Allow, Block, Allow and Promote, Promote, Prompt, Report  
**Write Action** – Does not apply to this type (not shown)

Execution Control rules are exactly what they sound like. They allow you to create a rule that responds in the way you choose when a file matching the rule attempts to execute. They do not have any effect on attempts to write (create, modify, or delete) matching files.

Execution Control rules are similar to Trusted Path rules, except that Execution Control rules allow you to specify a user or group and they offer more Execute Action options.

**Definition**

**Rule Type:** Execution Control

Select the action you want performed...

**Execute Action:** Allow

Files when executed from the following path(s)...

**Path Or File:**

Only when executed by the following process(es)...

**Process:** Any Process

Only when executed by a user matching the following user/group account(s)...

**User Or Group:** Any User

**Rule Applies To:**  All policies  
 Selected policies

For example, perhaps your developers use a tool called MyDevTool to develop and compile DLLs. The MyDevTool application is set up to run the DLLs it creates. You might create a rule that prevents this execution from being blocked.

Since the files created by MyDevTool are all DLLs, you can use **\*.dll** as your Path or File. If you were certain of the location of these files, you could further specify the path, but for this example we will leave the location open.

If you leave the Process field for this rule set to **Any Process**, any process on a client affected by the rule can run any DLL. To make this rule more secure, you might want to limit the right to execute files in this directory to MyDevTool application itself. To do this, you could use a macro to help specify the exact location of the tool, for example **<ProgramFiles>\ToolCo\MyDevTool\runtool.exe**.

If you have defined Active Directory groups, you might choose to further restrict the ability to run these DLLs to the group known to have permission to use this tool. To do this, you could choose **Specify User or Group...** on the User or Group menu and then enter the AD Group name for the permitted group, **Developers**, for example.

Now you have a rule that will allow execution of DLL files in any location as long as they are being executed by user in the Developers group using MyDevTool.

The screenshot shows the 'Add Custom Rule' dialog box with the following configuration:

- General:**
  - Name: Allow MyDevTool dll executions
  - Description: Allow standard developer tool to execute dlls it has compiled
  - Status:  Enabled  Disabled
  - Platform: Windows
- Definition:**
  - Rule Type: Execution Control
  - Execute Action: Allow
  - Path Or File: \*.dll
  - Process:  Any Process  Specific Process...  
<ProgramFiles>\ToolCo\MyDevTool\runtool.exe
  - User Or Group:  All Users  Specific User or Group...  
Developers
  - Rule Applies To:  All policies  Selected policies

Buttons: Save, Cancel

## File Creation Control

**Write Action Options** – Ignore, Block, Approve, Approve as installer, Prompt, Allow

**Execute Action** – Does not apply to this rule type (not shown)

File Creation Control rules allow you to control what happens when there as an attempt to write (create) a file that matches the rule. They do not have any effect on file execution attempts.

Like File Integrity Control rules, File Creation Control rules allow you to Block writes. However, File Creation Control rules allow you to specify a user or group and they offer more Write Action options for cases in which you are not blocking file writes.

The screenshot shows a configuration window for a File Creation Control rule. The fields are as follows:

- Rule Type:** File Creation Control
- Write Action:** Block (with a checked box for "Use Policy Specific Notifier")
- Path Or File:** (empty field with a browse button)
- Process:** Any Process
- User Or Group:** Any User
- Rule Applies To:** All policies (selected)

## Performance Optimization

**Write Action** – Ignore (value fixed for this rule type, not shown)

**Execute Action** – Does not apply to this rule type (not shown)

**Users** – Any User (value fixed for this rule type, not shown)

Unless instructed otherwise, the Bit9 Server keeps track of any files written to a computer running its agent. Normally, this is useful for monitoring purposes. However, there are cases in which a particular process writes many files to the same directory as part of its normal operation, and monitoring these write operations uses system and network resources unnecessarily while providing no important information. In cases such as these, you might choose to create a Performance Optimization custom rule for the uninteresting directory.

To create a rule that eliminates tracking for certain files, follow the instructions in [“Creating a Custom Rule”](#) on page 338 and choose **Performance Optimization** as the Rule Type. When you choose Performance Optimization, some other fields on the page change to reflect your choice. Note that although not shown, the Write Action for this rule is **Ignore**, meaning that writing of files matching this rule will not be tracked by the Bit9 Server.



Definition

Rule Type: Performance Optimization

Do not track files written to the following path(s)...  
(execution of these files will still be tracked and controlled)

Path Or File:

Only when written by the following process(es)...

Process: Any Process

Rule Applies To:  All policies  
 Selected policies

For example, perhaps an application called MyVirusGuard is writing a lot of temporary files to **c:\temp2\**.

You could create a Performance Optimization rule that specifies **c:\temp2\\*** in the Path or File field. The Bit9 Server would not track any files written to, modified in, or deleted from that location by anyone. This reduces processing and information collection, but it also means that you are not tracking *any* files being written to that directory.

If MyVirusGuard uses the executable MVGuard.exe for its operations, including writing files, you could add **\*\MVGuard.exe** to the rule as the Process, which lets MyVirusGuard write to the directory without tracking. The server continues to track files written to c:\temp2\ by any other process. Specifying the process allows you to accomplish the task you wanted while maintaining as much protection as possible. Note also that because you used the asterisk wildcard and a slash before the process name in the Process field, it does not matter where you installed MVGuard.exe – it is always allowed to write to the designated directory without tracking.

Add Custom Rule

General

Name: Ignore MyVirusGuard Writes

Description: Do not track any temporary files written by the MyVirusGuard application

Status:  Enabled  Disabled

Platform: Windows

Definition

Rule Type: Performance Optimization

Do not track files written to the following path(s)...  
(execution of these files will still be tracked and controlled)

Path Or File: c:\temp2\*

Only when written by the following process(es)...

Process: Specific Process...  
\*\MVGuard.exe

Rule Applies To:  All policies  
 Selected policies

Save Cancel

Since the (hidden) Execute Action for a Performance Optimization rule is **Default**, any *executions* in c:\temp2 are still tracked and executions are still blocked if other rules would block them – only file *writing* has been allowed and not tracked, and only if attempted by the process you specified.



## Pairing Ignore and Block Rules

In one previous example, a Process Exclusion was used to allow a specific process to write to the location normally blocked by the rule. You also can create an exclusion to a rule by pairing it with a second rule and ranking the exclusion rule above the main rule.

Perhaps a program called Super App has a log file called **superapp.log** in a **logs** subfolder. You might not want to create an exception for a process but instead only allow the files to be written in the particular subfolder while protecting the rest of the application folder. To do this, you could create two rules with the following characteristics:

- **Ignore Rule** – Create a Performance Optimization rule to ignore and allow writes (the automatic action choice) to **<ProgramFiles>\superapp\logs\\***
- **Block Rule** – Create a File Integrity Control rule with a Write Action of Block for the path **<ProgramFiles>\superapp\\***, and rank that rule lower than the Allow rule.

With the Performance Optimization rule ranked above the Block rule, Bit9 first checks to see whether a modification attempt matches the exception, and if it does, the Block rule is not evaluated.

Rank	Status	Rule Type	Name	Action	Path
1	Enabled	Performance Optimization	Allow Super App Log Writes	Ignore writes	c:\temp\superapp\logs\*
2	Enabled	File Integrity Control	Protect Super App Folder	Block writes	c:\temp\superapp\*



## Chapter 13

# Script Rules

This chapter describes Script Rules, which identify files to be tracked and managed as scripts by the Bit9 Security Platform. The Bit9 Server includes built-in script rules, and you can create custom rules to identify other scripts.

### Sections

Topic	Page
<a href="#">Overview</a>	376
<a href="#">Script Rules Priority vs. Other Bit9 Rules</a>	379
<a href="#">Policy Settings for Script Rules</a>	380
<a href="#">Creating a Custom Script Rule</a>	380
<a href="#">Editing a Script Rule</a>	383
<a href="#">Disabling or Deleting a Script Rule</a>	383
<a href="#">Viewing Rule Status on Computers</a>	384
<a href="#">Script Rule Examples</a>	385

## Overview

The Bit9 Security Platform tracks and manages two categories of files: *executables* and *scripts*. Executables are identified based on Bit9's analysis of their content. Scripts are identified by name.

### What is a Script?

A *script* is a file that contains executable or interpretable content that has meaning only in the context of a *script processor*. This dependency on a specific host process is what differentiates a script from typical executables. Script rules require two specifications:

- a *script type* file pattern definition to allow identification of the script file.
- a *script processor* specification that identifies the file that processes the script identified by the script type. You can either specify a string to match for the processor or, for Windows computers, let the File Association list on each agent computer determine the default processor for a file matching the script type. Only one processor may be specified for a script type, even if there are multiple compatible processors.

Examples of script files include VisualBasic scripts (\*.vbs), Batch scripts (\*.bat and \*.cmd), and shell scripts (\*.sh, \*.csh, etc.). Scripts might also be add-ons or extensions for browsers, such as Firefox XPI plug-ins and Chrome CRX extensions, or application data files such as Word documents (\*.docx). Examples of *script processors* include cmd.exe (Batch scripts), bash (shell scripts), wscript.exe (VisualBasic scripts), as well as processes that are not obviously script processors such as firefox.exe, chrome.exe and word.exe.

The script file and the processor are compared to rule specifications by string matching.

#### Notes

- File hashes are not used to identify scripts. Script files are hashed, but the script rule identifies a script by file extension.
- The Bit9 Security Platform monitors and controls scripts that use script and processor file names that can be identified and defined in a rule. Script processing that takes place in browser memory, such as with JavaScript, is not a candidate for control by Bit9 script rules.
- Certain scripts are identified by their content, and these may be subject to the rules for executables rather than the script rules. See [“Shell Scripts Identified by Content”](#) on page 379 for details.

### What Bit9 Script Rules Do

Script rules implement two types of action for files matching the rules:

- **Visibility:** When a file matching the script type in a rule is discovered, either because it is newly present on an agent computer or because a new rule was created, the file is added to the File Catalog and Files on Computers tables, and is tracked from that point forward. Although identified by name, a script file is hashed like other identified as “interesting” by Bit9, and its hash is stored in the file database.
- **Control:** When a file matching a script processor attempts to access a file identified as a script type in the same rule, that is considered a *script execution*. For enabled script

rules, script executions are controlled according to the policy settings for the computer on which the execution is attempted and any other applicable Bit9 rules.

The file state of a script identified by Bit9 depends upon when it was discovered and on the state of *Rescan Computers: Check to approve all existing scripts matching this definition*. If the *Rescan Computers* box is *not* checked, all scripts of the type identified by the rule are treated as unapproved when executed. If the *Rescan Computers* box is checked, script files currently on agent-managed computers at the time of the rescan are *locally approved* and (unless explicitly banned) allowed to execute under all Enforcement Levels. Script files discovered after the rescan are considered Unapproved, and their execution will be blocked at High or Medium Enforcement Levels.

## Pre-configured Script Rules

The Bit9 Security Platform includes several standard script rules, some of which are enabled by default. On the Script Rules page, you can enable or disable existing rules, modify the rules, and create new custom script rules.

Name	Type	Process	Enabled	Date Modified	Last Modified By
Linux Shell	*.sh (multiple)	/bin/bash (multiple)	Yes	Jul 30 2012 01:20:23 PM	System
Linux Perl	*.pl	/usr/bin/perl	Yes	Jul 30 2012 01:20:23 PM	System
Linux Python	*.py	/usr/bin/python	Yes	Jul 30 2012 01:20:23 PM	System
Mac Shell	*.sh (multiple)	/bin/bash (multiple)	Yes	Jul 30 2012 01:20:23 PM	System
Mac Perl	*.pl	/usr/bin/perl	Yes	Jul 30 2012 01:20:23 PM	System
Mac Python	*.py	/usr/bin/python	Yes	Jul 30 2012 01:20:23 PM	System
Mozilla Extensions	*.xpi	<File Association>	No	Jul 30 2012 01:20:23 PM	System
Chrome Extensions	*.crx	<File Association>	No	Jul 30 2012 01:20:23 PM	System
Ruby	*.rb	<File Association>	No	Jul 30 2012 01:20:23 PM	System
TCL	*.td	<File Association>	No	Jul 30 2012 01:20:23 PM	System
PowerShell	*.ps1 (multiple)	<File Association>	No	Jul 30 2012 01:20:23 PM	System
Python	*.py (multiple)	<File Association>	No	Jul 30 2012 01:20:23 PM	System
Perl	*.pl (multiple)	<File Association>	No	Jul 30 2012 01:20:23 PM	System
Java	*.class (multiple)	*\java.exe (multiple)	No	Jul 30 2012 01:20:23 PM	System
Visual Basic	*.vb (multiple)	<System>\cscrip.exe (multiple)	Yes	Jul 30 2012 01:20:23 PM	System
Registry	*.reg	<System>\reg.exe (multiple)	Yes	Jul 30 2012 01:20:23 PM	System
Batch	*.cmd (multiple)	<System>\cmd.exe (multiple)	Yes	Jul 30 2012 01:20:23 PM	System

Table 53 shows the standard script rules. Where the file extension is the same for different rules, the process, or process path, paired with the file extension is different.

**Table 53:** Standard Script Rules and File Extensions

Application or Category	Script Extensions	Processes	Platform	Default State
<b>Linux Shell</b>	.sh, .csh, .zsh, .ksh	/bin/bash, /bin/csh, /bin/ksh, /bin/sh, /bin/tcsh, /bin/zsh, /bin/dash, /bin/static-sh, /bin/busybox	Linux	Enabled
<b>Linux Perl</b>	.pl	/usr/bin/perl	Linux	Enabled
<b>Linux Python</b>	.py	/usr/bin/python	Linux	Enabled
<b>Mac Shell</b>	.sh, .csh, .zsh, .ksh	/bin/bash, /bin/csh, /bin/ksh, /bin/sh, /bin/tcsh, /bin/zsh	Mac	Enabled
<b>Mac Perl</b>	.pl	/usr/bin/perl	Mac	Enabled
<b>Mac Python</b>	.py	/usr/bin/python	Mac	Enabled
<b>Batch</b>	.cmd, .bat	<System>\cmd.exe <Systemx86>\cmd.exe	Windows	Enabled
<b>Registry</b>	.reg	<System>\reg.exe <Systemx86>\reg.exe <System>\regedt32.exe <Systemx86>\regedt32.exe <Windows>\regedit.exe <Systemx86>\regedit.exe>	Windows	Enabled
<b>Visual Basic</b>	.vbs, .vb, .vbe, .wsf, .wsh	<System>\cscript.exe, <Systemx86>\cscript.exe <System>\wscript.exe, <Systemx86>\wscript.exe	Windows	Enabled
<b>Java</b>	.jar, .class	*\java.exe, *\javaw.exe	Windows	Disabled
<b>Perl</b>	.pl, .pm	<File Association>	Windows	Disabled
<b>Python</b>	.py, .pyc, .pyo	<File Association>	Windows	Disabled
<b>PowerShell</b>	.ps1, .psm1	<File Association>	Windows	Disabled
<b>TCL</b>	.tcl	<File Association>	Windows	Disabled
<b>Ruby</b>	.rb	<File Association>	Windows	Disabled
<b>Chrome Extensions</b>	.crx	<File Association>	Windows	Disabled
<b>Mozilla Extensions</b>	.xpi	<File Association>	Windows	Disabled

## Script Rules Priority vs. Other Bit9 Rules

A script file defined by a Script Rule is also subject to any matching (non-script) Custom Rules, including those with actions that would Ignore writes, Block, Prompt or Report execution or writing, or Allow execution. For example, if a script file matches a Custom Rule with a Write Action of *Ignore*, the file state of the script will be Unapproved, and execution will be blocked at High or Medium Enforcement Levels. Also, if a script file and its processor match a Custom Rule with an Execute Action of Allow, the script will be allowed to execute regardless of its file state.

In addition, script files can be banned or approved by hash.

## Shell Scripts Identified by Content

The Custom Script Rules table includes rules for native Mac and Linux shell script files, and these are enabled by default. Although scripts are generally identified by file extension and processor in an explicit rule, there is an exception for Mac and Linux shell scripts.

Some shell scripts contain special markup in their first line that identifies the default interpreter that should be used to process them. This markup is usually referred to as *hashbang* or *shebang*, and consists of the “pound” or “hash” symbol (#) followed by an exclamation point (!). For example:

```
#!/bin/bash
```

indicates that the /bin/bash interpreter should be used to process this script file.

Because the shebang markup clearly identifies a file as “interesting” to Bit9, shell scripts with this markup are identified by content and tracked, regardless of whether there is a script rule for them. In effect, the markup creates an invisible script rule with the file as the script and the shebang markup identifying the processor.

How Bit9 rules are enforced on Mac and Linux shell scripts with the shebang pattern depends on how the script is run and whether any matching Custom Script Rule remains in effect:

- **Use the script as the command** – If a script file is run as a command, it will use the processor identified in the shebang, and will be subject to the policy settings that control *executables*, not *scripts*. An example of this might be:

```
$ ./foo.sh
```

Note that to run the script this way, the script itself must have execute permission in the operating system.

- **Use a defined processor/script combination as the command** – If a script file is run with the processor as the command and the script file as the argument, and if this combination is defined in the shebang or a Custom Script Rule, the action will be subject to the policy settings that control *scripts*. An example of this might be:

```
$ csh ./foo.sh
```

In this case, execution permission is not necessary for the script file.

- **Use an undefined processor/script combination** – If a script file is run with the processor that is not defined in a shebang pattern for the file nor in a Custom Script Rule, the script action is not controlled by the policy settings for *scripts*, even if the file itself has been identified as a script to track. This includes the case in which a script file includes a shebang pattern but a different processor is used to run it.

## Policy Settings for Script Rules

Unlike custom, registry, and memory rules, script rules do not specify an action. They function primarily to include files in a category already subject to tracking and action rules in the Bit9 Security Platform. Each policy has two Advanced Settings that specify how script files should be controlled on computers in that policy:

- **Block unanalyzed scripts and executables:** This setting determines whether scripts and executables not yet analyzed by the Bit9 Security Platform are blocked (e.g., in cases where initialization has not yet completed on a computer). It also provides a menu and links through which you can change or disable the notifier that appears if such files are blocked.
- **Block unapproved scripts:** This setting determines whether execution of scripts whose file state is Unapproved is blocked on computers with High or Medium Enforcement. It also provides a menu and links through which you can change or disable the notifier that appears if such files are blocked.

Also keep in mind that scripts are sometimes subject to the policy settings for executables instead of scripts. See [“Shell Scripts Identified by Content”](#) for more details.

### Related Topics

See [Table 20, “Advanced Setting Behavior,”](#) on page 158 for information on script-specific settings in policies.

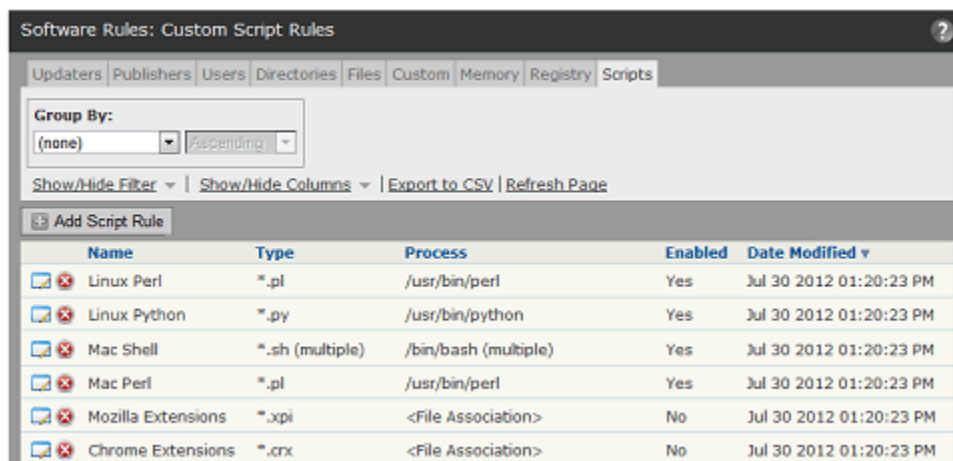
See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for information on configuring notifiers for blocked scripts.

## Creating a Custom Script Rule

The procedure below describes how to create a custom script rule. The rule parameters are shown in [Table 54](#).

### To add (create) a custom script rule:

1. In the console menu, choose **Rules > Software Rules**, and on the Software Rules page, click the **Scripts** tab. The Custom Script Rules table appears:



Name	Type	Process	Enabled	Date Modified
Linux Perl	*.pl	/usr/bin/perl	Yes	Jul 30 2012 01:20:23 PM
Linux Python	*.py	/usr/bin/python	Yes	Jul 30 2012 01:20:23 PM
Mac Shell	*.sh (multiple)	/bin/bash (multiple)	Yes	Jul 30 2012 01:20:23 PM
Mac Perl	*.pl	/usr/bin/perl	Yes	Jul 30 2012 01:20:23 PM
Mozilla Extensions	*.xpi	<File Association>	No	Jul 30 2012 01:20:23 PM
Chrome Extensions	*.crx	<File Association>	No	Jul 30 2012 01:20:23 PM



2. Click the **Add Script Rule** button. The Add Script Rule page appears.

3. In the Name field, enter the name you want to appear on the list of rules. You may also provide a longer, optional Description.
4. By default, a new script rule is **Enabled** when you configure it and click **Save**. If you want to enable the rule later, click **Disabled** in the Status field.
5. Choose a Platform: **Windows**, **Mac** or **Linux**. All script rules are platform-specific.
6. Choose a Script Definition, which determines how the script processor will be identified. See [Table 54](#) for the choices.  
**Platform Note:** For Mac or Linux scripts, only **Script Type and Process** is allowed.
7. For all Script Rules, enter one or more Script Types. A Script Type is the file name definition for this script type, usually the asterisk followed by a dot and the file extension. You can add script types by entering a pattern in the Script Type field, clicking the **Add** button to the right of the field, adding the next pattern, and so on.
8. For Script Type and Process rules (Windows only), you must also add one or more Script Processes. For each process in the rule, enter the process definition in the Script Process field, and click the **Add** button to the right of the field.
9. If you want to make sure all existing scripts matching this definition are added to the list of files tracked and controlled by the Bit9 Security Platform, check **Rescan Computers** box.
10. Click the **Save** button to save the rule. It should appear on the Script Rules page.

**Table 54:** Script Rule Parameters

Field	Description
<b>Name</b>	Name by which this rule is listed in the Script Rules table. (Required)
<b>Description</b>	Additional information about the rule. This can be any text you choose to enter. (Optional)
<b>Status</b>	Radio buttons that make this rule Enabled or Disabled. This allows you to create a rule that you use only at certain times, or to temporarily disable a rule without losing its definition.
<b>Platform</b>	Platform (Windows, Mac, or Linux) for which this script rule is defined. Each script rule must be specific to one platform.
<b>Script Definition</b>	<p>How you want to define the script rule. The menu choices are:</p> <p><b>File Association</b> – Choose this definition to allow the file association list on the agent computer to determine the Script Process. You still must provide the Script Type (file name).</p> <p>File Association might be a good choice for a common script type if your environment includes computers with different versions of the script engine for that type (for example, different versions of Perl). However, it is not necessarily the best choice when individual computers have multiple versions of the script engine; only the one identified in the File Association will be managed by Bit9. Consider your environment before making this choice.</p> <p><b>Platform Note:</b> Only Windows scripts can use File Association.</p> <p><b>Script Type and Process</b> – Choose this definition if you want to specify both the file patterns that define the script and the process that runs the script.</p>
<b>Script Type</b>	The file name pattern that determines whether a file matches this rule and is therefore considered a script. In most of the standard rules, the script type is defined by the file extension you want identified as a script (for example, *.vbs). You can use paths, wildcards, and macros in the script type. See <a href="#">“Specifying Paths and Processes”</a> on page 345 for a general description of pattern definitions options in Bit9 rules.
<b>Script Process</b>	The executable whose behavior you want to control when it processes files matching the Script Type. Examples of script processors include wscript.exe (Visual Basic scripts), cmd.exe (Batch scripts), ps.exe (PowerShell scripts) as well as processes that are not obviously script processors such as firefox.exe, chrome.exe and word.exe. You can use paths, wildcards, and macros in the script process. See <a href="#">“Specifying Paths and Processes”</a> on page 345 for a general description of pattern definition options in Bit9 rules
<b>Rescan Computers</b>	<p>If checked, rescans all connected computers running the Bit9 Agent to discover any files matching the script rule. If a matching file is found, it is added to the File Catalog with a file state of Approved. If not checked, all script files matching the rule are Unapproved. If a computer is disconnected, it will get the “rescan” rule once it reconnects, and will be re-scanned. Keep the following in mind:</p> <ul style="list-style-type: none"> <li>• Enabling Rescan Computers in a new or existing rule causes a delay during which existing local scripts might not be approved.</li> <li>• If a script file matches a custom rule that instructs the Bit9 Agent to ignore rules, it will continue to be ignored.</li> </ul>
<b>History</b>	For existing rules, a History panel appears at the bottom of the page, showing when and by whom the rule was created and last modified.

**Important**

Use of very broad definitions for either the Script Type or Script Process field is not recommended because of negative performance impact. If either field in a rules uses \* or \*.\* , a warning will be displayed on the page. Be as specific as possible in defining the file patterns in a Script Rule.

## Editing a Script Rule

You might choose to edit a script rule for a variety of reasons, including:

- enabling or disabling the script (see [“Disabling or Deleting a Script Rule”](#) on page 383 for more on the effects of enabling or disabling a script)
- adding, removing, or modifying patterns used to identify the script, or its processor
- changing the Script Definition to use File Association to identify the Script Processor, or to change from File Association to a specified processor pattern or patterns.

### To edit a script rule:

1. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. On the Software Rules page, click the **Scripts** tab. The Custom Script Rules table appears.
3. Click on the View Details (pencil and file) icon to the left of the rule you want to edit. The Edit Custom Script Rule page appears.
4. Edit the rule as you choose (see [Table 54](#) for a description of the parameters) and then click **Save**. The Edit Custom Rule page closes and the Custom Script Rules page is displayed.

## Disabling or Deleting a Script Rule

If you do not want a script rule to be effective anymore, you can either disable it, which leaves it in the table of script rules, or delete it from the table. In either case, the script rule stops affecting newly discovered files. However, any script file that was discovered while the rule was effective continues to be tracked by Bit9 and retains any file state assigned to it during the time the rule was enabled.

Disabling a script definition does not immediately remove the matching files from the inventory of files tracked by Bit9. This prevents loss of information if an action such as a rule change is taken accidentally. However, the exact amount of time a script file matching a disabled rule remains in inventory depends factors such as whether it is actually deleted from the agent or modified.

If a disabled definition is subsequently enabled with rescan enabled, only newly discovered scripts will be locally approved. Scripts that remained in the inventory will retain their previous state.

If you think you might use a rule again, disabling it temporarily is the best choice.

**To disable a script rule:**

1. In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Scripts** tab. The Custom Script Rules table appears.
2. Click the Edit button (pencil and file) next to the rule you want to disable. The Edit Script Rule page appears.
3. In the Status line, click the **Disabled** radio button, and then click the **Save** button at the bottom of the page. The rule is now disabled.

Deleting a rule eliminates it permanently – there is no undo or retrieval for a deleted rule. Because of that, be sure you actually want to delete the rule. Deletion of the rules that were pre-configured in Bit9 is not recommended.

**To delete a script rule:**

1. In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Scripts** tab. The Custom Script Rules table appears.
2. Click the Delete button (red circle with X) next to the rule you want to delete, and click **OK** on the confirmation dialog. The rule is now deleted.

## Viewing Rule Status on Computers

Depending upon the number of agents managed by your Bit9 Server and the number that are disconnected, not all agents might receive new or updated rules in a short amount of time. The Related Views menu on the Edit page for an enabled rule provides links to two different filtered views of the Computers page to help determine the status of the rule on agent-managed computers. The choices are:

- **All Computers that have received this rule**
- **All Computers that have not yet received this rule**

This menu does not appear for rules that have never been enabled.

## Script Rule Examples

The Bit9 Security Platform includes several pre-configured Script Rules. These are useful as examples for creation of other rules.

### Example: Windows Perl Scripts

One pre-configured Windows Script Rule will track and control executions of Perl scripts when enabled. On the Scripts tab on the Software Rules page, you can click on the Edit (pencil and file) button next to the Perl rule to see how it is defined.

The screenshot shows the 'Edit Custom Script' dialog box with the following details:

- General:**
  - Name: Perl
  - Description: (empty)
  - Status:  Enabled  Disabled
  - Platform: Windows
- Definition:**
  - Script Definition: File Association
  - Script Type: (empty)
  - Rescan Computers:  Check to approve all existing scripts matching this definition
- History:**
  - Created By: System
  - Date Created: Mar 21 2012 10:23:52AM
  - Last Modified By: System
  - Date Modified: Mar 21 2012 10:23:52AM

Buttons: Save, Cancel

The *Script Type* field includes two patterns – \*.pl and \*.pm. Any file ending in either of these extensions will be considered a Perl script file, and will be tracked by Bit9 once discovered.

The *Script Definition* field shows *File Association*. This means that you do not have to provide a pattern to match for the Script Processor. For each agent computer, this rule will use whatever the application file is identified as the Perl processor on that computer as the Script Processor. Any time the application associated with \*.pl or \*.pm files attempts to access those files, the agent will control execution based on the current state of the script file, the policy settings for the computer on which the execution attempt occurs, and any other rules affecting the files.

Notice that *Rescan Computers* is checked in this rule. This means that as soon as this rule is enabled, all computers managed by this Bit9 Server will be rescanned, and any files matching the Script Type for the rule will be locally approved and added to the File Catalog and Files on Computers list. When this box is not checked, all files of this script type are treated as unapproved. Other matching script files are “discovered” when an attempt to execute them occurs, and they are not locally approved, which might cause them to be blocked.

## Example: Windows Batch Scripts

The Bit9 Security Platform includes a script rule to identify and control executions of Windows batch scripts. On the Scripts tab of the Software Rules page, you can click on the Edit (pencil and file) button next to the Batch rule to see how it is defined.

The screenshot shows the 'Edit Custom Script' dialog box with the following details:

- General:**
  - Name: Batch
  - Description: (empty text area)
  - Status:  Enabled  Disabled
  - Platform: Windows
- Definition:**
  - Script Definition: Script Type and Process
  - Script Type: \*.cmd, \*.bat
  - Script Process: <System>\cmd.exe, <Systemx86>\cmd.exe
  - Rescan Computers:  Check to approve all existing scripts matching this definition
- History:**
  - Created By: System
  - Date Created: Jun 29 2012 03:29:54PM
  - Last Modified By: System
  - Date Modified: Jun 29 2012 03:29:54PM
  - CL Version: 2

Buttons at the bottom: Save, Cancel.

The *Script Type* field for the Batch rule includes two patterns – \*.cmd and \*.bat. Any file ending in either of these extensions will be identified as a Batch script file, and will be tracked by Bit9 once discovered.

The *Script Definition* field shows *Script Type and Process*, so it is necessary to provide at least one pattern to match for the Script Process. In this case, there are two processes listed so that *cmd.exe* is identified as the processor for this script for both 32-bit and 64-bit systems.

When this rule is enabled, any time the *cmd.exe* (in the locations shown) attempts to access a file with a .cmd or .bat extension, the agent will control execution based on the current approval state of the script file, the policy settings for the computer on which the execution attempt occurs, and any other rules affecting the files.

Because *Rescan Computers* is checked in this rule, as soon as the rule is enabled, all computers managed by this Bit9 Server will be rescanned, and any files matching the Script Type for the rule will be locally approved and added to the File Catalog and Files on Computers list.

## Example: Linux Shell Scripts

The Bit9 Server includes a script rule to identify and control executions of native shell scripts on Linux computers. On the Scripts tab of the Software Rules page, you can click on the Edit (pencil and file) button next to the Linux Shell rule to see how it is defined.

**Edit Custom Script**

**General**

Name: Linux Shell

Description:

Status:  Enabled  Disabled

Platform: Linux

**Definition**

Script Definition: Script Type and Process

Script Type:

- \*.csh
- \*.zsh
- \*.ksh

Script Process:

- /bin/bash
- /bin/csh
- /bin/ksh

Rescan Computers:  Check to approve all existing scripts matching this definition

**History**

Created By: System

Date Created: Aug 2 2012 07:39:23 PM

Last Modified By: System

Date Modified: Aug 2 2012 07:39:23 PM

CL Version: 14

Save Cancel

The *Script Type* field for the Linux Shell rule includes several patterns – \*.sh, \*.csh, \*.zsh, \*.ksh. Any file ending in one of these extensions will be identified as shell script file, and will be tracked by the Bit9 Server once discovered.

The *Script Definition* field shows *Script Type and Process*, which is the only choice usable for Mac and Linux rules. There is a long list of processes in the rule, which support native script processing on the supported Linux platforms. If you choose you can add or remove processors (or script types) for this rule.

When this rule is enabled, any time a listed processor, such as /bin/bash, attempts to access a file with a listed extension, such as .sh, the Bit9 Server will control execution based on the current approval state of the script file, the policy settings for the computer on which the execution attempt occurs, and any other rules affecting the files.

Because *Rescan Computers* is checked in this rule, as soon as the rule is enabled, all computers managed by this Bit9 Server will be rescanned, and any files matching the Script Type for the rule will be locally approved and added to the File Catalog and Files on Computers list.





## Chapter 14

# Registry Rules

This chapter describes Registry Rules, which control what happens when there is an attempt to make changes in the Windows Registry at locations that match paths you specify. If you choose, you can limit the rules to specified users and/or processes.

**Platform Note:** Registry rules affect only computers running Windows operating systems.

### Sections

Topic	Page
<a href="#">Overview</a>	390
<a href="#">Specifying the Notifier for Registry Rules</a>	391
<a href="#">Creating Registry Rules</a>	391
<a href="#">Registry Rule Parameters</a>	394
<a href="#">Specifying Registry Paths</a>	397
<a href="#">Specifying Processes in Registry Rules</a>	398
<a href="#">Rule Ranking</a>	402
<a href="#">Disabling or Deleting Registry Rules</a>	403
<a href="#">Sample Registry Rules</a>	404
<a href="#">Autostart Rules</a>	406

## Overview

Registry rules enable you to block, report, allow, or prompt the user for a choice when there are attempts to write to Windows Registry locations matching paths you specify. Creation, modification and deletion of keys or values all count as “writes”.

You can view a list of registry-rule-related events, including any blocks caused by registry rules, by going to the Events page and choosing Registry on the Saved Views menu

### Notes

For computers in Visibility mode policies, registry rules that would block writing or prompt users for a decision are treated as report-only rules, and therefore will not block or prompt.

## Rule Scope

You can create registry rules that apply to all users and all processes that try to make a registry change on any Windows computer. You also can create a more focused scope for a rule by specifying one or more of the following criteria:

- **Process-specific** – You can make a rule apply only when *certain processes* attempt to write to the specified location.
- **User- or group-specific** – You can make the rule apply only to a particular *user or group of users*.
- **Policy-specific** – You can choose to limit a rule to *computers in specified policies*.
- **Rule order** – Registry rules are evaluated in order of *Rank*, a column that is displayed by default on the Registry Rules table. The rule ranked ‘1’ has the highest rank, ‘2’ is next, and so on. You can change the order of rules. For example, you can create a rule that applies when *a particular user* attempts to access a specified Registry path, and put that above a rule that applies when *any other user* attempts to access that path.

### Important

Registry rules generally should be as narrowly targeted as possible to avoid unintended effects.

## Sample Rules

A new installation of Bit9 Server is pre-configured with built-in registry rules, disabled by default, which you can view by clicking the Registry tab on the Software Rules page. Some of these are samples that you may either enable as is or use as a guide to creating your own rules. The Autostart rule, which also is disabled by default, protects a long list of registry locations potentially affected on startup. See the section “[Sample Registry Rules](#)” on page 404 for an example of how a rule can be configured.

## Exporting and Importing Registry Rules

You can export registry rules from one server and import them to another. There are buttons for this purpose on the Registry Rules page. See “[Exporting and Importing Rules](#)” on page 359 in the Custom Rules chapter for more information.

## Specifying the Notifier for Registry Rules

The Bit9 Agent provides *notifiers* that can be displayed when a rule blocks an action or prompts the user for a decision to allow or block an action. For each registry rule, you can choose from two sources for the notifier:

- **Use Policy Specific Notifier** – Each Policy includes an Advanced Setting, “Enable registry rules”, which is always on. This setting has a Notifier field in which you can specify the notifier that appears on agent computers when a registry rule blocks an action. The policy setting also allows you to choose <none> in case you do not want a notifier for registry rules in a policy, including those that should prompt. You can assign the policy-specific notifier to any registry rule. See [“Advanced Settings”](#) on page 156 for more information.
- **Custom Notifier** – If you do not choose the policy-specific notifier, you can choose (or create) a notifier specifically for a registry rule. The choices appear on a menu on the Add/Edit Registry Rule page. Custom Notifiers for Prompt rules must have a notifier. Custom Notifiers for Block rules allow you to choose <none> so that no notifier appears.

See [Table 55](#) below for the registry rule notifier settings. See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for more on notifiers.

## Creating Registry Rules

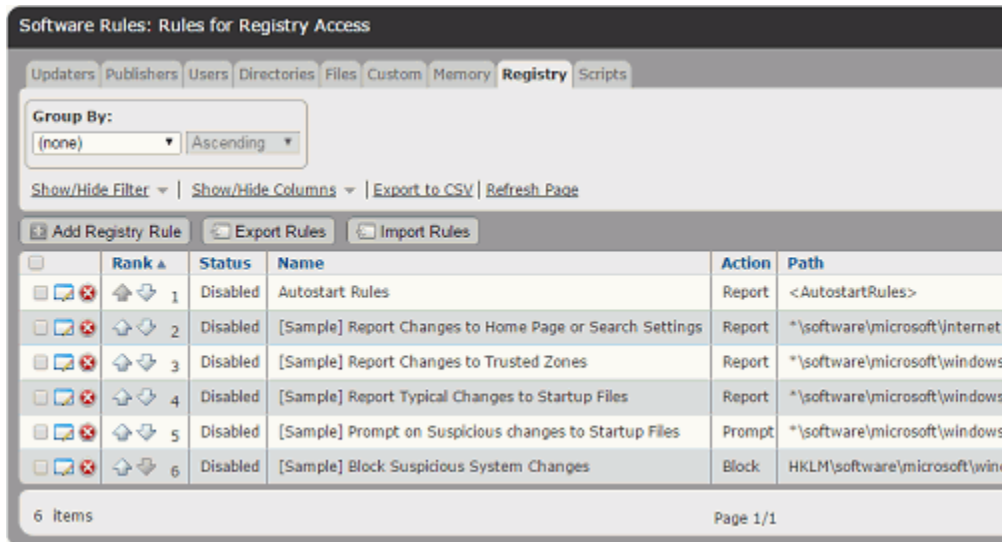
In addition to providing a name, to create a registry rule, you need to provide the information shown in bold in the left column of the table below and enter it in the Add Registry Rule page in the locations on the right:

General Description	Field on Add/Edit Registry Rule Page
If <b>this/these source process(es)</b> ...	Process
...and/or <b>this/these user(s)</b> ...	User or Group
... attempt to modify the Windows Registry at <b>this/these location(s)</b> ...	Registry Path
... on computers in <b>this/these policy(ies)</b> ...	Rule applies to:
.. then <b>this action</b> should be taken.	Write Action

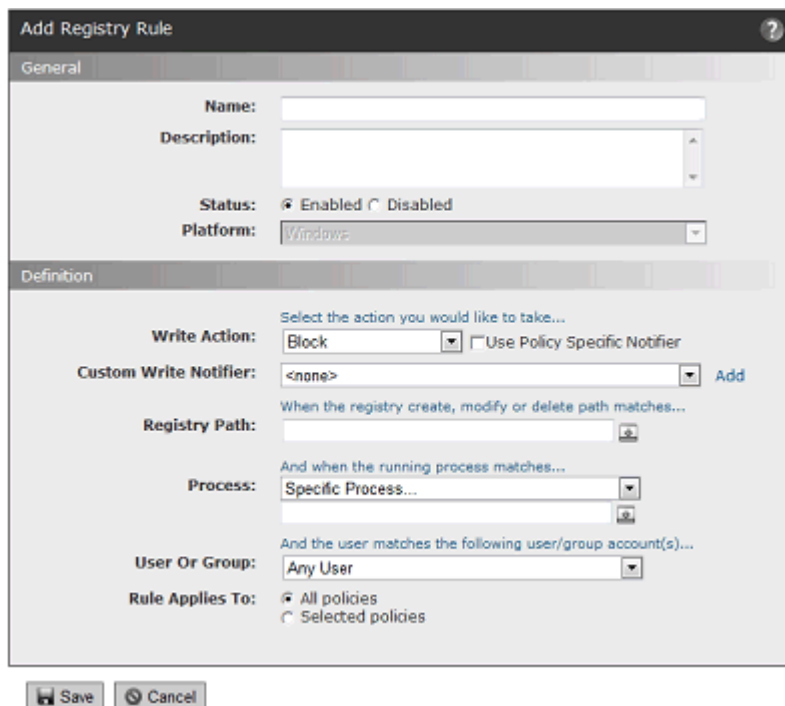
For each of these parameters, there could be multiple matching items, or the rule could specify all items in that class (for example, the rule applies to all users, or all policies, or all source processes).

**To add (create) a registry rule:**

1. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click **Registry Rules**, either on its tab or in the menu to the left of the page. The Registry Rules page appears:



3. To create a new rule, click the **Add Registry Rule** button. The Add Registry Rule page appears.



4. In the Name field, enter the name you want to appear on the list of rules.

5. If you want to add other comments about the rule, such as its purpose or its relationship to other rules, you may provide an optional Description.
6. By default, a new registry rule is **Enabled**. If you want to delay enabling the rule, click **Disabled** in the Status field.
7. Enter the remaining information you want for this rule (see [Table 55, “Registry Rule Parameters,”](#) on page 394) and then click the **Save** button. The newly created rule is listed at the *bottom* of the Registry Rules table and temporarily highlighted in yellow. If your Registry Rules table is more than one page long, the view shifts to the last page so you can see the new rule.
8. If you want to change the priority of this rule, use the arrows in the Rank column, or drag-and-drop, to move it down to the desired rank. See [“Rule Ranking”](#) on page 402 for more details.

## Registry Rule Parameters

Table 55 shows the parameters available on the Add/Edit Registry Rule page.

**Table 55:** Registry Rule Parameters

Field	Description
<b>Name</b>	Name by which this rule is identified in the Registry Rules table. (Required)
<b>Description</b>	Optional information about the registry rule. This can be any text you choose to enter.
<b>Status</b>	Radio buttons that make this rule Enabled or Disabled. This allows you to create a rule that you use only at certain times, or to temporarily disable the rule without losing the information used to create it.
<b>Platform</b>	Platform for which this rule is effective. This is a read-only field and the value is always Windows. Registry rules do not have any impact on non-Windows platforms.
<b>Write Action</b>	The action to take when there is a write attempt matching this rule. See Table 56 for the action options. For all Windows platforms except Windows Server 2003 64-bit, write rules also control changes to registry permissions.
<b>Use Policy Specific Notifier</b>	If you choose Block or Prompt as the Write Action, this checkbox appears to the right of the Write Action choice. If you check the box, the notifier that appears when a registry rule blocks an action is the notifier specified for the Enable Registry Rules setting in the policy for the computer on which the action was blocked. If not checked, you can choose a custom notifier from the Custom Write Notifier menu.
<b>Custom Write Notifier</b>	If you choose Block or Prompt as the write action, and you do not check the Use Policy Specific Notifier box, this menu appears.  If you choose Block as the write action, you can choose any notifier from the menu. The menu also includes a <none> option so that you can disable the notifier for this rule.  If you choose Prompt as the write action, you can choose any notifier on the menu. Prompt rules must display a notifier, so there is no <none> choice in this case.
<b>Registry Path</b>	Registry path to which this rule applies. See “ <a href="#">Specifying Registry Paths</a> ” on page 397 for details on your options for specifying the path.

Field	Description
<b>Process</b>	This menu allows you to limit the rule so that it is applied only when certain processes attempt to execute or write files matching the path specification. See <a href="#">“Specifying Processes in Registry Rules”</a> on page 398 for details on specifying a process and <a href="#">Table 57</a> for process menu options.
<b>User or Group</b>	This menu allows you to specify users or groups to which this rule applies. See <a href="#">“Specifying Users or Groups”</a> on page 402 for details on specifying users or groups.
<b>Rule applies to</b>	The radio button for this rule allows you to apply the rule to <b>All policies</b> or <b>Selected policies</b> . If you choose <b>Selected policies</b> , a list of all policies available on your Bit9 Server appears, each with a checkbox. You can check as many policies as you choose.
<b>History</b>	For existing rules, a History panel shows when and by whom the rule was created and modified.

## Specifying a Write Action

The Write Action in a registry rule is the action to take when there is a registry write attempt matching this rule. [Table 56](#) shows the options. Write action includes creation, deletion and modification of registry keys on all platforms. It also includes changes to registry permissions on all Windows platforms except Windows Server 2003 64-bit.

**Table 56:** Write Action Menu Options

Option	Description
<b>Block</b>	<p>Prevent creation, deletion and modification of registry keys and values at locations matching this rule.</p> <p>When Block is chosen, the Use Policy Specific Notifier checkbox and a Custom Write Notifier menu appear. These allow you to specify the notifier, if any, that appears when the rule blocks an action. See <a href="#">Table 55</a> for more details.</p>
<b>Prompt</b>	<p>Present a notifier dialog to the computer user when an attempt to modify the registry is made at this location. The dialog choices are Block or Allow. Once the user responds to the dialog, the choice applies anytime the same process matches the same rule on the same computer with the same user – the user will not be prompted again in this case.</p> <p>When Prompt is chosen, the Use Policy Specific Notifier checkbox and a Custom Notifier menu appear. These allow you to specify the notifier that appears to prompt the user. See <a href="#">Table 55</a> for more details.</p>
<b>Report</b>	<p>Do not block modifications at this registry path but report them as Bit9 events.</p>
<b>Allow</b>	<p>Allow creation, deletion and modification of registry keys and values at locations matching this rule. This is the default behavior if there is no rule for a path.</p> <p>Use of Allow gives you a way to create an exception to a more general rule that blocks at a particular location. For example, if you create a rule that blocks all writes to</p> <pre>*\Software\MyApp\*</pre> <p>you could create an exception by creating a higher ranking rule that allows writes to</p> <pre>*\Software\MyApp\SpecialKey</pre>



## Specifying Registry Paths

The Registry Path specifies the locations in the Windows Registry to which a rule applies.

The image shows a configuration window for a registry rule. At the top, it says "When the registry create, modify or delete path matches...". Below this is a text box labeled "Registry Path:" followed by an empty input field and a small icon. Below that, it says "And when the running process matches...". This is followed by a dropdown menu labeled "Process:" which currently shows "Specific Process...". Below the dropdown is another empty input field with a small icon.

All registry paths must begin with one of the following strings:

- **HKLM\**
- **HKCU\**
- **HKLM-SoftwareX86\**
- **HKLM-SoftwareX64\**
- **HKCU-SoftwareX86\**
- **HKCU-SoftwareX64\**
- **\*\**

### Notes

- You cannot use macros in the Registry Path.
- If you enter a path that uses a key that is actually a link to other keys, the rule will not work. For example, a rule that uses a path containing *CurrentControlSet* will fail to work. You might consider using wildcards in place of the linked item (for example, *ControlSet\** in the previous case).

## Using Wildcards

You can use wildcards (“\*” for zero or more characters, “?” for one character) in the Registry Path. You can use wildcards to specify partial paths or multiple paths in the registry. The number of wildcards in a path is not restricted.

You can use wildcards to skip a level and make a rule apply to values (or sub-keys) of a sub-key, even if you don’t know their names. For example:

```
*\myapp\*\*
```

applies the rule only to keys or values *below a sub-key* of *myapp*, such as

```
HKLM\myapp\apprunner\4.0
```

but it does not apply to sub-keys or values in *myapp* itself, such as

```
HKLM\myapp\sharedfiles
```

**Caution**

When you use wildcards, do not to create a rule that is so broad that it will interfere with activity that is required for legitimate use by an application or the operating system. Do not use the asterisk wildcard by itself in the Registry Path field, especially with rules that block all writes, unless you are certain it will not interfere with necessary operations on the agent computer. Registry rules may seriously impact the performance of an application or system.

**Specifying Keys or Values**

If a path ends with a "\", it matches only the key at that path. If a path ends in "\\\*", the rule applies to all keys, sub-keys and values underneath that path.

If a path ends without a slash or wildcard, it applies only to a value (not a key) matching the path. For example:

```
HKLM\SOFTWARE\FileReader\9.0\ViewOutput
```

would match a *value* named "ViewOutput" but not a *key* named "ViewOutput"

You can add more than one path to a Registry Rule. See [“Entering Multiple Paths or Processes”](#) on page 401 for details. In the Registry Rule table, rules with more than one path show the first path in the Registry Path field followed by **(multiple)**.

**Specifying Processes in Registry Rules**

The Process field on the Add/Edit Registry Rule page allows you to fine-tune the rule according to the process – that is, the running file – attempting to modify the registry.

The screenshot shows a web form for configuring a registry rule. At the top, it says "When the registry create, modify or delete path matches...". Below this is a "Registry Path:" label followed by a text input field and a small icon. Underneath, a red box highlights a section titled "And when the running process matches...". This section contains a "Process:" label followed by a dropdown menu currently showing "Specific Process..." and a small icon.

You can make the rule effective for all processes, certain types of processes, specific processes, or all processes except the one(s) you name. [Table 57](#) shows the Process options.

**Table 57:** Process Menu Options

Menu Option	Description
<b>Any Process</b>	Applies the rule to any process that attempts to write to the registry.
<b>Any Promoted Process</b>	Applies the rule to any process that is promoted at the time the rule is evaluated. A promoted process is any approved process that is marked as an installer, or has been promoted as a consequence of a custom rule, or is an approved process launched by a promoted process.
<b>Any System Process</b>	Applies the rule to every process that is running under the security context of the Local System user. This choice has the same effect as choosing Local System in the User or Group menu, but may be more efficient.
<b>Specific Process...</b>	Opens a text box below the menu; you can enter the names of processes you want controlled by this rule. See <a href="#">“Specifying Processes in Registry Rules”</a> on page 398 for the guidelines and requirements for specifying a process.
<b>Any Process Except...</b>	Opens a text box below the menu, in which you can enter processes you <i>do not</i> want controlled by this rule. See <a href="#">“Specifying Processes in Registry Rules”</a> on page 398 for the guidelines and requirements for specifying a process.  <b>Note:</b> If you specify a User or Group and also choose Any Process Except from the process menu, the rule is enforced <i>unless the exception process is being executed by the user or group</i> .

When you choose a Process option that requires entry of a path (either *Specific Process...* or *Any Process Except ...*), you have several options for defining paths:

- **Specify a specific process or a directory** – You can enter a process specification that exactly identifies a process by path and name so that only that file matches the rule. You also can enter a specification that identifies a directory, which matches all processes in that directory and its subdirectories.
- **Specify a local drive or UNC path** – You can identify a local process by using a local drive name, such as *C:\folder1\subfolder\application.exe*. You also can enter a remote process by using a UNC path, such as *\\computername\dir\application.exe*. Mapped drives in a path or process specification are not recognized.
- **Use wildcards** – You can use wildcards (‘?’ for any one character and ‘\*’ for zero or more characters) to expand the scope of a process specification or help you match a file or folder whose exact location you don’t know. Wildcards may be used at the beginning, end or middle of a path.
- **Use macros** – You can use special Bit9 macros to identify certain well-known folders in the Microsoft Windows environment, even if you don’t know their exact location on all agent computers.
- **Specify multiple process paths** – You can add more than one process definition per rule.

## Specifying Processes or Directories

You can choose to enter a directory or a specific file as your process path. When you specify a directory, you are instructing the rule to apply when any process in that directory or in any of its subdirectories attempts to write to the registry location specified (unless there are higher-ranked rules that match the current process).

To indicate that a Process definition is a directory, you must end it with a backslash (\) or a backslash and asterisk (\\*). If you do not include the backslash, the rule will attempt to match a *file* by the name you provided, not a directory. For example, either of the following correctly identifies “subfolder2” as a directory in a process definition:

```
c:\folder1\subfolder2\  
c:\folder1\subfolder2\*
```

However, the following is *not* recognized as a directory:

```
c:\folder1\subfolder2
```

If you use path macros in a process definition, the expanded macro is treated as a directory, even if you don’t follow it with a backslash. See [Using Macros](#).

## Using Wildcards

You can use wildcard characters in the Process field. Asterisk (\*) indicates zero or more characters and question mark (?) indicates one character. You can also use them to specify processes that appear in different locations on different computers (although macros might be a more effective way to accomplish this – see [Using Macros](#)).

The number of wildcards in a process specification is not restricted. For example, you could define a path as:

```
*\Win*\folder?\
```

## Automatic Process Path Conversions

The Process field undergoes automatic path conversions if it contains certain symbols:

- A process path that ends with a slash has the ‘\*’ wildcard added at the end of the path.
- A process path with no slash or drive letter has “\*\” added at the beginning of the path.
- Drive letters may be used in a path as long as they are for local fixed volumes. Mapped drive letters should not be used because there is no guarantee that the mapping exists on all computers.
- The string “\*:\” applies to all attached storage volumes except for floppy disks and CD-ROMs.

## Specifying Devices in Process Path

You can specify that a rule applies when writes are attempted by processes running from some or all devices on the agent computer by including `\device\` in the path. For example:

- `\device*\` specifies all devices.
- `\device\harddisk*\` specifies attached storage volumes except for floppy disks and CD-ROMs.
- `\device\cdrom*\` specifies CD-ROM devices.

## Using Macros

You can use certain macros in the Process field of a Registry Rule. You can see a menu of macros by typing the left angle bracket (<) character in the Process field. There are two types of macro supported in Registry Rule processes:

- **Path macros** – These are a subset of the well-known folders in the Microsoft Windows environment, and they always identify a location rather than a specific file. A path macro can be used only at the *beginning* of a Path or File specification in a rule (i.e., with no other text before it in the string).
- **Registry macros** – These are macros that specify strings in the Windows Registry. A registry macro can be used anywhere in the Path or File specification.

Macros can be an effective way to define a rule that works on all Windows computers even when the files you want to affect are in different locations on different computers.

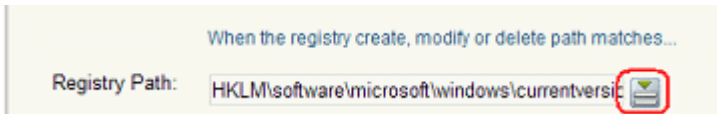
See “[Using Macros](#)” on page 347 of the Custom Rules chapter for a description of path and registry macros. These macros may be used in the Process field of a registry rule.

### Notes

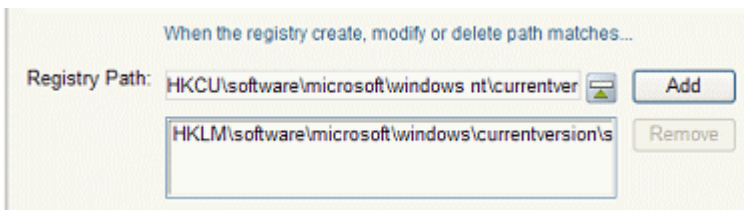
Macros may be used in the Process field of a Registry Rule but not in the Registry Path field.

## Entering Multiple Paths or Processes

For both the Registry Path and the Process field in a rule, you can enter more than one string. For example, when you have entered the first Registry Path for this rule, click the Expand button to the right of the box.

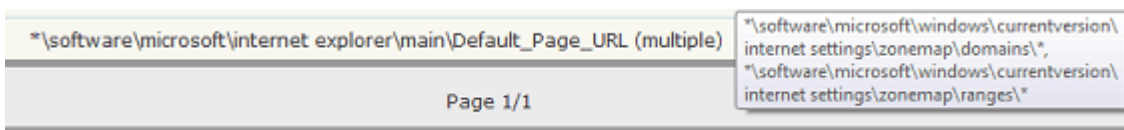


You can then add additional paths by typing them in the box and clicking **Add** after each one.



You can remove any path by clicking the Expand button, selecting the file or path in the list below the Registry Path box, and clicking the **Remove** button. Adding or removing items in the Process field works in a similar way.

If you enter multiple paths or processes for a rule, the Registry Rules page shows the first path and then **(multiple)** in the relevant column for this rule. Moving the mouse over the value shows a tooltip with the complete list of paths or processes for the rule.



## Specifying Users or Groups

You can create a rule that applies only when specific users or users in specific groups attempt an action. The choices for User or Group on the Add/Edit Custom Rule page are:

- **Any Users** – applies the rule to all users.
- **Specific User or Group...** – opens a text box below the menu, into which you can enter AD users or groups in the format *userorgroupname@domain* or *domain\userorgroupname*
- The other menu choices are built-in Windows groups, such as **Authenticated Users** and **Local Administrators**.

### Notes

- When running on Windows Vista and later, membership in pre-defined security groups like Administrators requires that the application run as an administrator. If a group definition is necessary for a rule, consider using security groups you have defined rather than the pre-defined groups
- There is a brief delay after a user logs in before group membership is established and group-based rules become effective. This delay may be longer if you have a large number of rules. If you need a rule to be effective as soon as possible after a user logs on, do not specify a user *group* in the rule. Rules that specify a *username* or *SID* are always active and won't be affected by this delay.

## Rule Ranking

Registry rules have a “Rank” number and are evaluated from lowest number to highest number, beginning with the rule ranked ‘1’. By default, rules appear in their rank order, but you can re-sort the table by other columns if you choose. If a path location matches two different rules, the highest ranking rule (that is, the one with the lowest number), takes precedence and the lower-ranked (higher number) rule has no effect. There is one exception to this behavior – rules whose action is Report do not stop processing of lower ranked rules.

You can change the ranking of rules.

### To change the rank of a registry rule:

1. On the Registry Rules page, if the rules are not currently sorted by rank, click on the Rank column head to sort them.
2. Find the rule whose rank you want to change.
3. To give the rule a higher rank, click the up arrow button next the to rule until it is ranked where you want it to be.

**-or-**

Move the mouse cursor over the rule you want to move, hold down the left mouse button, drag the rule to the new location, and release the mouse button.

- To give the rule a lower rank, click the down arrow next to the rule until it is ranked where you want it to be, use the drag-and drop method to move the rule.

Rank ▲	Name	Path
1	[Sample] Block Suspicious System Changes	HKLM\software\microsoft\windows nt\currentversion\image file
2	[Sample] Report Changes to Trusted Zones	"\software\microsoft\windows\currentversion\internet settings\
3	[Sample] Prompt on Suspicious changes to Startup Files	"\software\microsoft\windows\currentversion\policies\explorer\
4	[Sample] Tamper Protection	HKLM-SoftwareX86\microsoft\windows nt\currentversion\image
5	[Sample] Tamper Protection	HKLM-SoftwareX86\microsoft\windows nt\currentversion\image
6	[Sample] Tamper Protection	HKLM-SoftwareX86\microsoft\windows nt\currentversion\image

### Note

When using drag-and-drop, you cannot drag rules between pages. If you need to move a rule to a ranking not currently shown, you can increase the number of rows shown per page by using the menu at the bottom right corner of the Custom Rules page.

## Disabling or Deleting Registry Rules

If you do not want a registry rule to be effective anymore, you can either disable it, which leaves it in the registry rules table, or delete it from the table. In either case, the rule stops affecting newly discovered files. However, files that were affected by the rule before it was disabled retain any file state assigned to them by the rule.

If you think you might use the rule again, disabling it temporarily is the best choice.

### To disable a registry rule:

- In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Registry** tab. The Registry Rules table appears.
- Click the Edit button (pencil and file) next to the rule you want to disable. The Edit Registry Rule page appears.
- In the Status line, click the **Disabled** radio button, and then click the **Save** button at the bottom of the page. The rule is now disabled.

Deleting a rule eliminates it permanently – there is no undo or retrieval for a deleted rule. Because of that, be sure you actually want to delete the rule.

### To delete a registry rule:

- In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Registry** tab. The Registry Rules table appears.
- Click the Delete button (red circle with X) next to the rule you want to delete, and click **OK** on the confirmation dialog. The rule is now deleted.

## Viewing Rule Status on Computers

Depending upon the number of agents managed by your Bit9 Server and the number that are disconnected, not all agents might receive new or updated rules in a short amount of time. The Related Views menu on the Edit page for an enabled rule provides links to two

different filtered views of the Computers page to help determine the status of the rule on agent-managed computers. The choices are:

- **All Computers that have received this rule**
- **All Computers that have not yet received this rule**

This menu does not appear for rules that have never been enabled.

## Sample Registry Rules

The Bit9 Security Platform is shipped with a series of disabled sample registry rules. You can examine the rules to see whether you might want to enable them, or to consider using them as templates that you modify to accomplish exactly what you want for your own registry protection.

### **Important**

Do not enable any of the sample registry rules without examining their parameters, including which registry paths they apply to and what action (Block, Prompt, Report, Allow) they involve. You also can configure the Action for a rule to Report for a period of time before you make it fully active (i.e., blocking, prompting or allowing actions).

### **Example: Report Changes to Internet Explorer Trusted Zone**

The example here starts with parameters from the sample rule “[Sample] Report Changes to Trusted Zones”, which is included in the rules shown in the console but disabled by default. This rule reports changes to the sites or IP addresses in the Internet Explorer Trusted Zone on machines running the Bit9 Agent. Because you may give higher privileges to sites in the trusted zone, any changes to that zone could be a security risk.



To begin the process, go to the **Registry** tab and then click on the View Details (pencil on file) button next to the “[Sample] Report Changes to Trusted Zones” rule.

**Edit Registry Rule**

**General**

**Name:** [Sample] Report Changes to Trusted Zones

**Description:** Generate an event whenever a change is made to the sites or IP addresses in the Internet Explorer Trusted Zone

**Status:**  Enabled  Disabled

**Platform:** Windows

**Definition**

**Write Action:** Report

**Registry Path:** When the registry create, modify or delete path matches...

\*\software\microsoft\windows\currentversion\internet settings\zonemap\domains\  
\*\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\  
Add Remove

**Process:** Any Process

**User Or Group:** Any User

**Rule Applies To:**  All policies  Selected policies

**History**

**Created By:** System  
**Date Created:** Mar 28 2012 11:01:37AM  
**Last Modified By:** System  
**Date Modified:** Mar 28 2012 11:01:37AM

Save Cancel

As the description says, this rule generates a Bit9 Event whenever a registry change is made that will change the sites or IP addresses in the Internet Explorer Trusted Zone. The parameters are:

- **Write Action: Report** – This indicates that the rule only reports changes matching the rule – it does not block an action or allow an action that would otherwise be blocked. If you wanted to create a more restrictive rule, you could change this to **Prompt**, in which case each user on a computer running the Bit9 Agent would have the opportunity to block or allow Registry changes matching the rule. Or you could **Block** any changes matching the rule.
- **Registry Path:**
  - \*\software\microsoft\windows\currentversion\internet settings\zonemap\domains\  
\*\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\  
– This rule includes two paths. Because the paths starts with \*, any attempt to write to them, whether it starts with HKCU, HKLM, or another allowed prefix, will match the rule. Because the paths end with a slash and asterisk, keys and values at and below **domains** and **ranges** (respectively) will match the rule.
- **Process: Any Process** – Any process attempting registry writes that match the other parameters activates the rule.
- **User or Group: Any User** – Any user attempting registry writes that match the other parameters activates the rule.

- **Rule applies to: All policies** – All policies, and therefore all Windows computers running the Bit9 Agent, are subject to this rule.

If you enable this rule, registry write attempts matching the rule appear on the Events page. You can search for them by clicking the Show/Hide Filters button on the Events page and creating a filter for “Subtype is Report write (registry rule)”. When you find an event report matching this rule, you might respond in one of several different ways:

- If the change is undesirable, undo the change (outside of Bit9) and create a new rule preventing that change from happening again (rather than just reporting it). Use wildcards or multiple paths to make the rule as narrow or broad as necessary.
- Allow the change if you consider it benign or desirable.
- Use the file information on the Bit9 Server to obtain information about the process that has attempted the modification.

## Autostart Rules

The table of Registry Rules for Bit9 Security Platform v7.2.1 includes an Autostart Rules rule that is actually a collection of rules. It is disabled by default. When activated, this rule set reports and optionally blocks attempts to modify registry locations that control what happens when you startup a computer. For example, one of the many paths covered by the Autostart Rules is:

**HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**

If you want to test the impact of this set of rules before making it active, you can choose Report on the Write Action menu for the rule. Then, after some time has elapsed, you can go to the Events page and filter for “Rule name contains Autostart” to see what events have been triggered by this rule set. If you determine that activating the rule will not interfere with your operations, you can change the Write Action value to Block (or Prompt).

On the Edit Registry Rule page for Autostart Rules, the Registry Path is shown as <AutostartRules>. This macro refers to the current list of locations controlled by this rule. The list is maintained within the Bit9 Server and not enumerated in the rule definition. It is expected to be updated and expanded with future releases. If you need more detail about specific locations affected by this rule in your version, please contact Bit9 Technical Support.

### Note

Pre-7.0 releases of Bit9 (Parity) had Registry Rules that affected a small subset of the locations included in the new Autostart Rules set. If you used any of these startup rules, you might want to use the Autostart Rules instead for greater protection on startup.

## Chapter 15

# Memory Rules

This chapter describes Memory Rules, which can protect a process from being accessed or altered by other processes.

**Platform Note:** Memory rules affect only computers running Windows operating systems.

**Sections**

Topic	Page
<a href="#">Overview</a>	408
<a href="#">Specifying the Notifier for Memory Rules</a>	409
<a href="#">Creating Memory Rules</a>	409
<a href="#">Memory Rule Parameters</a>	411
<a href="#">Specifying Target and Source Processes</a>	415
<a href="#">Rule Ranking</a>	419

## Overview

Memory Rules allow you to monitor attempts to access a process on a Windows computer, and if you choose, protect the process from being accessed or altered by any other process(es) or user(s). When a rule matches your criteria, you can *block* read, write or execution access to a matching process, *report* on access, or *prompt* the user on the agent system to block or allow access. There also are advanced options for special cases.

If an in-memory malicious attack occurs on a system protected by the Bit9 Agent, a properly configured memory rule can prevent that attack from spreading to other processes, or even from accessing information in other processes. Memory rules limit the vulnerability of a protected computer. They can also protect specific applications or processes from termination or other manipulation by users or malicious code.

You can view a list of memory-rule-related events, including blocked actions caused by memory rules, on the Events page by choosing **Memory** on the Saved Views menu.

### Important

There are two built-in rules named *Tamper Protection*, ranked 1 and 2 by default, that help protect agent computers. Do not edit these rules, and do not disable or reorder them unless instructed to do so by Bit9 Support. Check the description field for any rule before you consider modifying it.

## Rule Scope

You can create memory rules that apply to all Windows computers, regardless of which user and what process attempts to access the process you specify. You also can create a more focused scope for a rule by specifying one or more of the following criteria:

- **Source-process-specific** – You can make a rule apply only when a particular source process attempts to access the target process you are monitoring or protecting.
- **User- or group-specific** – You can make the rule apply only to a particular user or group of users.
- **Policy-specific** – You can choose to limit a rule to computers in specified policies.
- **Rule order** – Memory rules are evaluated in order of *Rank*, a column that is displayed by default on the Memory Rules table. The rule ranked ‘1’ has the highest rank, ‘2’ is next, and so on. You can change the order of rules to have a more specific rule evaluated before a more general one. For example, you can create a rule that applies when *a particular user* attempts to access a process, and put that above a rule that applies when *any other user* attempts to access the process. See [“Rule Ranking”](#) on page 419 for more details.

There are certain restrictions on where memory rules are effective:

- A memory rule cannot be used to protect a process from itself. For example, you cannot create a rule that prevents a process from terminating itself, or from modifying its own memory.
- Memory Rules are not supported on Mac or Linux computers, or computers running Windows Server 2003 64-bit.
- Kernel Memory Access rules are supported only on computers running Windows XP or Windows Server 2003 *without* SP1.

- Dynamic Code Execution rules are supported only on Windows computers running 32-bit operating systems.
- For computers in Visibility mode policies, memory rules that would block writing or prompt users for a decision act as report-only rules, and do not block or prompt.

## Exporting and Importing Memory Rules

You can export memory rules from one server and import them to another. There are buttons for this purpose on the Memory Rules page. See [“Exporting and Importing Rules”](#) on page 359 in the Custom Rules chapter for more information.

## Specifying the Notifier for Memory Rules

The Bit9 Agent provides *notifiers* that can be displayed when a rule blocks an action or prompts the user for a decision to allow or block an action. For each memory rule, you can choose from two sources for the notifier:

- **Use Policy Specific Notifier** – Each Policy includes an Advanced Setting, “Enforce memory rules”, which is always on. This policy setting has a Notifier field in which you can specify the notifier that appears on agent computers when memory rules block an action. The policy setting also allows the choice of <none> to have no notifier for memory rules in that policy, include those that should prompt. You can assign the policy-specific memory rule notifier to any memory rule. See [“Advanced Settings”](#) on page 156 for more information.
- **Custom Notifier** – If you do not choose the policy-specific notifier, you can choose (or create) a notifier specifically for a memory rule. The choices appear on a menu on the Add/Edit Memory Rule page. Custom Notifiers for Prompt rules must have a notifier. Custom Notifiers for Block rules allow you to choose <none> so that no notifier appears.

See [Table 58](#) below for the memory rule notifier settings. See [Chapter 17, “Block Notifiers and Approval Requests,”](#) for more on notifiers.

## Creating Memory Rules

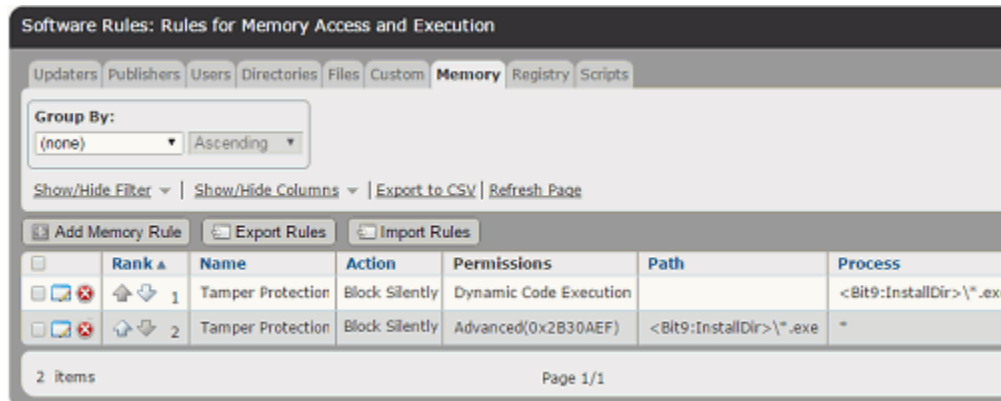
In addition to providing a name, to create a memory rule, you need to provide the information shown in bold in the left column of the table below and enter it in the Add Memory Rule page in the locations on the right:

General Description	Field on Add/Edit Memory Rule Page
If <b>this/these source process(es)</b> ...	Source Process
...and/or <b>this/these user(s)</b> ...	User or Group
... attempt the following <b>memory access type</b> ...	Permissions
... to <b>process(es) at this/these location(s)</b> ...	Target Process
... on computers in <b>this/these policy(ies)</b> ...	Rule applies to:
... then <b>this action</b> should be taken.	Action

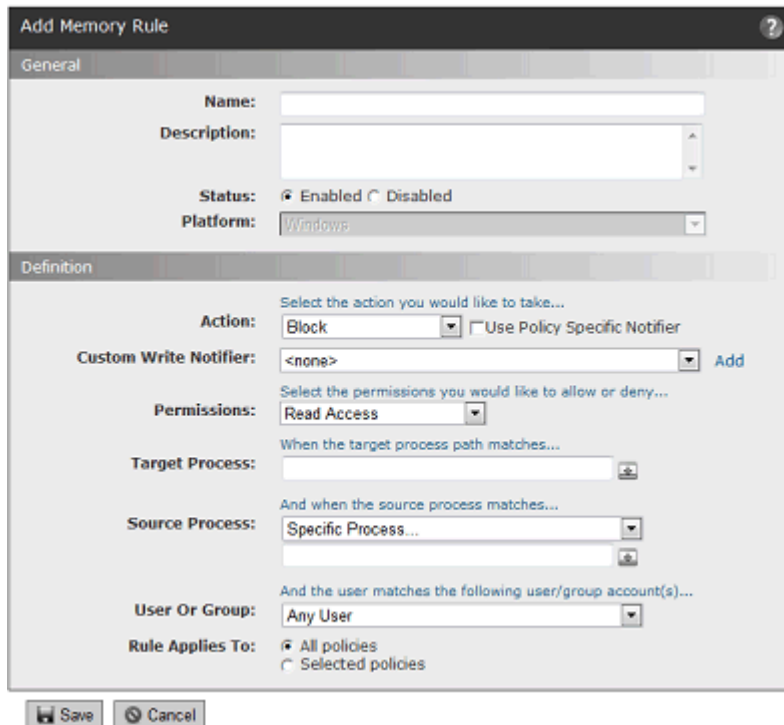
Each of these parameters could have multiple matching items, or the rule could specify *all* items in that class (e.g., the rule applies to all users, or all policies, or all source processes).

**To add (create) a memory rule:**

1. In the console menu, choose **Rules > Software Rules**. The Software Rules page appears.
2. Click **Memory** on the left menu or the tab on the page. The Memory Rules table appears, showing several built-in rules and any other memory rules that have been created on your server.



3. Click the **Add Memory Rule** button. The Add Memory Rule page appears.



4. In the Name field, enter the name you want to appear on the list of rules. You may also provide a longer, optional description.

5. By default, a new memory rule is **Enabled**. If you want to delay enabling the rule, click **Disabled** in the Status field.
6. Enter the remaining information you want for this rule (see [Table 58, “Memory Rule Parameters”](#) on page 411) and then click the **Save** button. The newly created rule is listed at the *bottom* of the Registry Rules table and temporarily highlighted in yellow. If your Registry Rules table is more than one page long, the view shifts to the last page so you can see the new rule.
7. If you want to change the priority of this rule, sort the Memory Rules table by Rank and use the arrows in the Rank column (or drag-and-drop) to move the rule to the desired rank. See [“Rule Ranking”](#) on page 419 for more details.

## Memory Rule Parameters

[Table 58](#) shows the parameters available on the Add/Edit Memory Rule page.

**Table 58:** Memory Rule Parameters

Field	Description
<b>Name</b>	Name by which this rule is identified in the Memory Rules table. (Required)
<b>Description</b>	Optional information about the memory rule. This can be any text you choose to enter.
<b>Status</b>	Radio buttons that make this rule Enabled or Disabled. This allows you to create a rule that you use only at certain times, or to temporarily disable the rule without losing the information used to create it.
<b>Platform</b>	Platform for which this rule is effective. This is a read-only field and the value is always Windows. Memory rules do not have any impact on non-Windows platforms.
<b>Action</b>	The action you want the Bit9 Agent to take when there is an attempt to access or alter a process matching this rule. <a href="#">Table 59</a> shows the options for this field.
<b>Use Policy Specific Notifier</b>	If you choose Block or Prompt as the Action, this checkbox appears to the right of the Action choice. If you check the box, the notifier that appears when a memory rule blocks an action is the notifier specified for the Enforce Memory Rules setting in the policy for the computer on which the action was blocked. If not checked, you can choose a custom notifier from the Custom Write Notifier menu.
<b>Custom Write Notifier</b>	If you choose Block or Prompt as the Action, and you do not check the Use Policy Specific Notifier box, this menu appears. When Block is the Action, you can choose any notifier from the menu. The menu also includes a <none> option so that you can disable the notifier for this rule. When Prompt is the Action, you can choose any notifier on the menu. However, Prompt rules <i>must</i> display a notifier, so there is no <none> choice in this case.

Field	Description
<b>Permissions</b>	The type of access you want to affect with this rule. <a href="#">Table 60</a> shows the permissions options.
<b>Target Process</b>	The process(es) you want this rule to restrict, monitor, or allow access to. See <a href="#">“Specifying Target and Source Processes”</a> on page 415 for a description of the ways you can define a target process.
<b>Source Process</b>	This menu allows you to apply the rule only when a specified Source Process requests access to the Target Process. <a href="#">Table 61</a> , <a href="#">“Source Process Menu Options,”</a> on page 418 shows the menu choices. <a href="#">“Specifying Target and Source Processes”</a> on page 415 describes options for entering a path. <b>Note:</b> No Target Process specification is needed for Kernel Memory Access or Dynamic Code Execution rules because the Source Process applies the rule to itself.
<b>User or Group</b>	This menu allows you to specify users or groups to which this rule applies. See <a href="#">“Specifying Users or Groups”</a> on page 418 for detail on specifying users or groups.
<b>Rule applies to</b>	The radio button for this rule allows you to apply the rule to <b>All policies</b> or <b>Selected policies</b> . If you choose <b>Selected policies</b> , a list of all policies available on your Bit9 Server appears, each with a checkbox. You can check as many policies as you choose.
<b>History</b>	For existing rules, a History panel appears at the bottom of the page, showing when and by whom the rule was created, and when and by whom it was last modified.



## Specifying the Rule Action

The Action for a Memory Rule defines what you want Bit9 to do if there is a memory access attempt matching the rule. [Table 59](#) shows the options.

**Table 59:** Action Menu Options

Field	Description
<b>Block</b>	<p>Prevent access to, termination of, or modification of processes matching this rule.</p> <p>When Block is chosen, the Use Policy Specific Notifier checkbox and a Custom Write Notifier menu appear. These allow you to specify the notifier, if any, that appears when the rule blocks an action. See <a href="#">Table 58</a> for more details.</p>
<b>Block Silently</b>	<p>Prevent access to, termination of, or modification of processes matching this rule. Do not display a notifier, and do not generate a Bit9 event.</p>
<b>Prompt</b>	<p>Present a notifier dialog to the endpoint user when there is an attempt to access, terminate, or modify processes matching this rule. The dialog choices are Block or Allow. Once the user responds to the dialog, the choice applies anytime the same process matches the same rule on that computer – the user will not be prompted again in this case.</p> <p>When Prompt is chosen, the Use Policy Specific Notifier checkbox and a Custom Write Notifier menu appear. These allow you to specify the notifier that appears to prompt the user. See <a href="#">Table 58</a> for more details.</p> <p><b>Note:</b> Use of Prompt as the action for Dynamic Code Execution rules is <i>not recommended</i> because the combination can have destabilizing effects on computers running the Bit9 Agent.</p>
<b>Report</b>	<p>Do not block access, termination, or modification of matching processes but report the actions as Bit9 events.</p>
<b>Allow</b>	<p>Allow all memory/process operations that match this rule. This is the default behavior if there is no rule for a particular target or source process.</p> <p>Use of Allow gives you a way to create an exception to a more general rule that blocks at a particular location. For example, if you create a rule that blocks all memory operations at</p> <pre>c:\Program Files\InterestingApp\*</pre> <p>you could use Allow to create a higher ranking rule that allows operations at</p> <pre>c:\Program Files\InterestingApp\Subfolder\</pre>

## Specifying the Rule Permissions

Permissions define the type of access you want to affect with this rule, such as read, write or execution. Some options allow you to control multiple types of access. [Table 60](#) shows the options available on the permissions menu.

**Table 60:** Permissions Menu Options

Field	Description
<b>Control Process</b>	Access required to control the execution of a process or thread, including the ability to terminate the process.
<b>Read Access</b>	Access required to retrieve, copy or duplicate certain information about a process or thread. If all you are concerned about is data loss or theft, you might use this choice with the Block Action.
<b>Write Access</b>	Access required to modify a process or thread and its attributes.
<b>Dynamic Code Execution</b>	Affects whether an application can execute code not associated with an executable image. This protection prevents arbitrary or floating code execution of the sort used by many forms of malware. Protects against attempts to disable Dynamic Execution Protection (DEP). Applies only to 32-bit systems. <b>Important:</b> Do not create a Dynamic Code Execution rule with <b>Prompt</b> as the action choice – this could cause undesirable results on agent computers.
<b>Kernel Memory Access</b>	Affects whether a user-mode process can access kernel memory. You can create rules allowing access by a legitimate application while denying access for all other applications. Applies only to Windows XP and Windows Server 2003 (without SP1).
<b>Write + Control</b>	Both write and control permissions. You can use this Permission choice and choose Block as the Action to prevent an attack on a process, such as a malicious code injection, termination, or other alterations.
<b>Read + Write + Control</b>	Read, write, and control permissions. This is the option you would use, along with the Block Action, to prevent data loss or theft as well as attacks. This does not include Dynamic Code Execution or Kernel Memory Access.
<b>Advanced...</b>	This option allows for very detailed control of memory access. Contact Bit9 Technical Support before using the Advanced option.

## Specifying Target and Source Processes

You usually specify two processes in a memory rule:

- **Target Process** – The process(es) you want the rule to restrict, monitor, or allow access to.
- **Source Process** – The process(es) requesting access to the Target Process.

When you specify Target Process in a Memory Rule, you have several options for defining the string for that parameter. These same options can be used when you choose one of the two Source Process options that require entry of a path (*Specific Process...* or *Any Process Except ...*). These options are:

- **Specify a directory or a process** – You can enter a process specification that exactly identifies a file by path and name so that only that file matches the rule. You also can enter a specification that identifies a directory, and so affects processes running from files in that directory and its subdirectories.
- **Specify a local drive or UNC path** – You can identify a process by using a local drive name, such as *C:\folder1\subfolder\application.exe*. You also can enter a remote process by using a UNC path, such as *\\computer\dir\application.exe*. Mapped drives in a path or process specification are not recognized.
- **Use wildcards** – You can use wildcards ('?' for any one character and '\*' for zero or more characters) to expand the scope of a process specification or help you match a file or folder whose exact location you don't know. Wildcards may be used at the beginning, end or middle of a path.
- **Use macros** – You can use special Bit9 macros to identify certain well known folders in the Microsoft Windows environment, even if you don't know their exact location on all agent computers.
- **Specify multiple paths or processes** – You can add more than one process path definition per rule.

### Specifying a File or Directory

You can specify a directory or a file as the Target or Source Process path. Using a directory applies the rule to processes in that directory and any of its subdirectories (unless higher-ranked rules apply to processes or subdirectories in it).

To identify a Process definition as a directory, you must end it with a backslash (\) or a backslash and asterisk (\\*). Without the backslash, the rule will attempt to match a *file* by the name you provided, not a directory. For example, either of the following correctly identifies a directory in a process definition:

```
c:\folder1\subfolder2\  
c:\folder1\subfolder2\*
```

However, the following is not recognized as a directory:

```
c:\folder1\subfolder2
```

If you use path macros in a process definition, the macro is treated as a directory, even if you don't follow the it with a backslash. See [Using Macros](#).

## Using Wildcards

You can use wildcard characters in the Process fields. Asterisk (\*) indicates zero or more characters and question mark (?) indicates one character. You can use wildcards to specify partial paths or multiple paths for directories that appear in different locations on different computers (although macros might be a more effective way to accomplish this – see [Using Macros](#)). Wildcards are not allowed inside of macros.

The number of wildcards in a process specification is not restricted. For example, you could define a path as:

```
*\Win*\folder?\
```

### Caution

When you use wildcards, be careful not to create a rule that is so broad that it will interfere with activity that is required for legitimate use by an application or the operating system. Don't use the asterisk wildcard by itself in Target Process field, especially with rules that block multiple types of access, unless you are absolutely certain it will not interfere with necessary operations on the agent computer.

## Automatic Path Conversions

When a rule is processed, file paths in a process field undergo several automatic path conversions if they contain certain symbols:

- Any path that ends with a slash has the '\*' wildcard added at the end of the path.
- Any path that has no slash or drive letter has "\*" added at the beginning of the path
- Drive letters may be used in a path as long as they are for local fixed volumes. Mapped drive letters should not be used because there is no guarantee that the mapping exists on all computers.
- The string ".\*:" applies to all attached storage volumes except for floppy disks and CD-ROMs.

## Specifying Devices in Paths

You can create rules that apply to processes on some or all devices on the agent computer by including `\device\` in the path. For example:

- `\device*\` specifies all devices.
- `\device\harddisk*\` specifies attached storage volumes except for floppy disks and CD-ROMs.
- `\device\cdrom*\` specifies CD-ROM devices.

## Using Macros

You can use certain macros in the Process fields. You can see a menu of macros by typing the left angle bracket (<) character in either of the Process fields. There are two types of macros supported in Memory Rule processes:

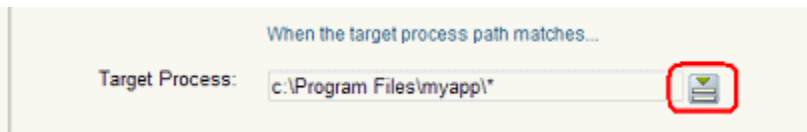
- **Path macros** – These are a subset of the well known folders in the Microsoft Windows environment, and they always identify a location rather than a specific file. A *path* macro can be used only at the beginning of a Path or File specification in a rule (i.e., with no other text before it in the string).
- **Registry macros** – These are macros that specify strings in the Windows Registry. A *registry* macro can be used anywhere in the Path or File specification.

Macros can be an effective way to define a rule that works on all agent computers even when the processes you want to specify are in different locations on different computers.

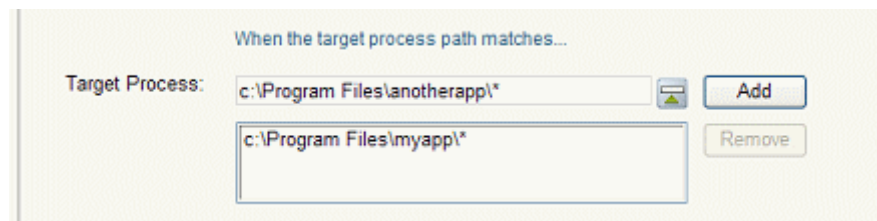
See “Using Macros” on page 347 of the Custom Rules chapter for a description of path and registry macros. The macros described there may be used in the Process fields of a memory rule.

## Entering Multiple Target or Source Processes

For each Process field in a Memory Rule, you can enter more than one string. For example, when you have entered the first Memory Path for a rule, click the Expand button to the right of the box.



You can then add process paths by typing them in the box and clicking **Add** after each one.



You can remove any process path by clicking the Expand button, selecting the path in the list below the box, and clicking the **Remove** button.

If you enter multiple paths in either process field in a rule, the Memory Rules table shows the first path and then “(multiple)” in the relevant column for this rule. Moving the mouse over the value shows a tooltip with the complete list of processes for the rule.



## The Source Process Menu

The Source Process field in a Memory Rule specifies the process that is requesting access to the Target Process. The Source Process menu includes options that are completely defined by your menu choice, such as **Any Process**, and options that require entry of a path to the process(es):

**Table 61:** Source Process Menu Options

Field	Description
<b>Any Process</b>	Applies the rule to any process that attempts to access the target process.
<b>Any Promoted Process</b>	Applies the rule to any source process that is promoted at the time the rule is evaluated. A promoted process is any approved process that is marked as an installer, or has been promoted as a consequence of a custom rule, or is an approved process launched by a promoted process.
<b>Any System Process</b>	Applies the rule to every source process that is running under the security context of the Local System user. This has the same effect as choosing Local System in the User or Group menu.
<b>Specific Process...</b>	Opens a text box below the menu, into which you can enter source process(es) you want controlled by this rule.
<b>Any Process Except...</b>	Opens a text box below the menu, into which you can enter the source process(es) you <i>do not</i> want controlled by this rule. <b>Note:</b> If you specify a User or Group and also choose Any Process Except from the process menu, the rule is enforced <i>unless the exception process is being executed by the user or group</i> .

## Specifying Users or Groups

You can create a rule that applies only when specific users or users in specific groups attempt an action. The choices for User or Group on the Add/Edit Memory Rule page are:

- **Any Users** – applies the rule to all users.
- **Specific User or Group...** – opens a text box below the menu, into which you can enter AD users or groups in the format *userorgroupname@domain* or *domain\userorgroupname*

- The other menu choices are built-in Windows groups, such as **Authenticated Users** and **Local Administrators**.

### Notes

- When running on Windows Vista and later, membership in pre-defined security groups like Administrators requires that the application run as an administrator. If a group definition is necessary for a rule, consider using security groups you have defined rather than the pre-defined groups
- There is a brief delay after a user logs in before group membership is established and group-based rules become effective. This delay may be longer if you have a large number of rules. If you need a rule to be effective as soon as possible after a user logs on, do not specify a user *group* in the rule. Rules that specify a *username or SID* are always active and won't be affected by this delay.

## Rule Ranking

Memory rules have a “Rank” number and are evaluated from lowest number to highest number, beginning with the rule ranked ‘1’. By default, rules appear on the Memory Rules page in their rank order, but you can sort the table by other columns if you choose.

If a memory-related action matches a rule’s definition, that rule is evaluated. Rule processing continues down the rank order to see whether any other rules match the current memory-related action. If there is another match, what happens next depends on the *Permissions* setting for the rules:

- If the action matches two rules, but these rules have different permissions settings – for example, one is applied to *Read Access* and the other is applied to *Write Access* – both rules are evaluated. In this case, if there is a third matching rule that is applied to *Control Process*, that rule is also evaluated.
- If the action matches two (or more) rules and all have *the same* permissions settings – for example, both are applied to *Write Access* – only the first rule is evaluated. There is one exception to this behavior – a rule whose action is Report does not stop processing of lower ranked rules with the same permissions setting.

You can change the ranking of rules if you decide that you want one of your rules to be considered before its current rank position.

### Important

There are two built-in rules named *Tamper Protection*, ranked 1 and 2 by default, that help protect the server. Do not rank other rules higher than these unless instructed to do so by Bit9 Technical Support.

### To change the rank of a memory rule:

1. On the Memory Rules page, if the rules are not currently sorted by rank, click on the Rank column head to sort them.

2. Find the rule whose rank you want to change.
3. To give the rule a higher rank, click the up arrow button next to the rule until it is ranked where you want it to be.  
**-or-**  
 Move the mouse cursor over the rule you want to move, hold down the left mouse button, drag the rule to the new location, and release the mouse button.
4. To give the rule a lower rank, click the down arrow next to the rule until it is ranked where you want it to be, or use the drag-and drop method to move the rule.

	Rank ▲	Name	Action	Permissions	Path
	1	Tamper Protection	Block Silently	Dynamic Code Execution	
	2	Tamper Protection	Block Silently	Advanced(0x2B30AEF)	<Bit9:InstallDir>\*.exe
	3	Prompt if Writing to Test	Prompt	Write Access	test.exe

## Disabling or Deleting Memory Rules

If you do not want a memory rule to be effective anymore, you can either disable it, which leaves it in the memory rules table, or delete it from the table. In either case, the rule is no longer effective.

If you think you might use the rule again, disabling it temporarily is the best choice.

### To disable a memory rule:

1. In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Memory** tab. The Memory Rules table appears.
2. Click the Edit button (pencil and file) next to the rule you want to disable. The Edit Memory Rule page appears.
3. In the Status line, click the **Disabled** radio button, and then click the **Save** button at the bottom of the page. The rule is now disabled.

Deleting a rule eliminates it permanently – there is no undo or retrieval for a deleted rule. Because of that, be sure you actually want to delete the rule.

### To delete a memory rule:

1. In the console menu, choose **Rules > Software Rules**, and when the Software Rules page appears, click the **Memory** tab. The Memory Rules table appears.
2. Click the Delete button (red circle with X) next to the rule you want to delete, and click **OK** on the confirmation dialog. The rule is now deleted.

## Viewing Rule Status on Computers

Depending upon the number of agents managed by your Bit9 Server and whether any are disconnected, not all agents might receive new or updated rules in a short amount of time. The Related Views menu on the Edit page for an enabled rule provides links to two different filtered views of the Computers page to help determine the status of the rule on agent-managed computers. The choices are:



- **All Computers that have received this rule**
- **All Computers that have not yet received this rule**

This menu does not appear for rules that have never been enabled.



## Chapter 16

# Event Rules

This chapter describes Event Rules, which allow you to specify an action to be performed when an event matches filters you define.

### Sections

Topic	Page
<a href="#">Overview</a>	424
<a href="#">Enabling, Disabling, and Deleting Event Rules</a>	425
<a href="#">Disabling Processing of All Event Rules</a>	426
<a href="#">Testing a Rule before Enabling</a>	427
<a href="#">Creating and Editing Event Rules</a>	428
<a href="#">Sample Event Rules</a>	438

## Overview

Event Rules allow you to specify an action to be performed when a file- or computer-related event occurs that matches filters you define. To use this feature, a console user must have *Manage event rules* permission. See [“Account Group Permissions”](#) on page 93.

You can create an alert that reports when a specified event rule is triggered. See [“Creating Alerts”](#) on page 498.

## Events That Can Trigger Rule Actions

Only events that relate to files can be used to trigger an event rule. Each rule is required to have one event subtype specified; for example, the rule might specify that its action is triggered when an event with the subtype *New file on network* occurs. You may add more subtypes so that the rule takes action under several different event conditions. You also may add other specifications to the rule, such as that the event included a reference to a particular IP address.

You also may add specifications that the rule only runs when the target file identified in the event, or its parent process, has certain properties. For example, you might specify that a new, unapproved file is uploaded to an analysis service only if it does not have Bit9 SRS reputation approval enabled.

## Actions A Rule Can Take

The following actions can be taken using Event Rules:

- **Change global file state** – An Event Rule can create a global Approval or Report Ban, and can remove a global Approval or Ban for a file referenced in an event. This may be done for all computers or by policy. In addition, the optional ability to create a fully functional Ban via Event Rules may be activated. Rules that change global state may also be configured to resolve related approval requests from endpoint users.
- **Change global process state** – An Event Rule can create a global Approval or Report Ban, and can remove a global Approval or Ban for the file of the process referenced in an event. This may be done for all computers or by policy. In addition, the optional ability to create a fully functional Ban via Event Rules may be activated. Rules that change global state may also be configured to resolve related approval requests from endpoint users.
- **Change local file state** – An Event Rule can create or remove a Local Approval for a file referenced in an event. Rules that change local state may also be configured to resolve related approval requests from endpoint users.
- **Upload file** – An Event Rule can initiate upload of a file referenced in an event to the Bit9 Server.
- **Analyze file** – An Event Rule can initiate upload of a file to any analysis service configured through the Bit9 Connector.
- **Move computer** – Optionally, a computer referenced in a file-related event may be moved to a different policy and Enforcement Level.

Users will only see action options for which they have permission. For example, users without permission to submit files for analysis will not see the *Analyze file* option.

## Simulating the Effect of a Rule

An important feature of Event Rules is the ability to simulate what would happen if you fully enabled a rule without actually taking the action specified. Event rules can have a significant impact on the Bit9 Server, and if not configured properly, they may have undesirable and unintended results. Because of this, it is strongly recommended that any new rule be run in *Simulate only* mode before it is fully enabled – this is one of the options on the Add and Edit Event Rule pages. See “[Testing a Rule before Enabling](#)” on page 427 for a recommended work-flow using Simulate only.

## Re-Applying a Rule to Past Events

Bit9 also provides the ability to apply a new rule to past events. This can be useful in combination with Simulate only mode, allowing you to apply the rule to a larger set of past events to see the events that *would have been* processed by the rule. You can then review these results, and you may choose to fine tune the rule to reduce the conditions under which the rule is triggered. You might also re-apply a new rule to past events when it is fully enabled if, for example, you want to send all new, unapproved files that have appeared in the past week to an external service for analysis.

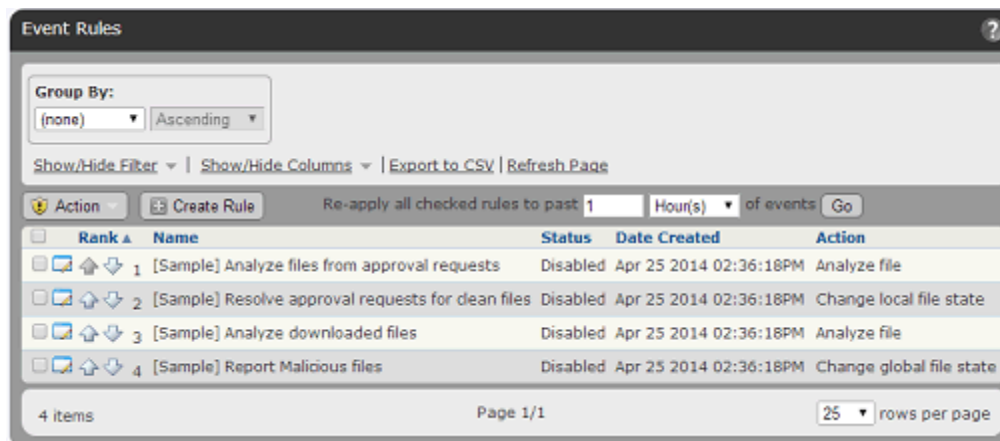
## Enabling, Disabling, and Deleting Event Rules

You can enable, disable, or delete specific Event Rules on either the Event Rules (table) page or the Edit Event Rule page.

On the Event Rules page, you can select one or more rules and either enable or disable them using the Action menu. Note that you cannot choose the Simulate Only option on this menu. To enable a rule in Simulate Only mode, use the Edit Event Rule page.

### To enable or disable rules in the Event Rules table:

1. On the console menu, choose **Rules > Event Rules**. The Event Rules page appears, showing the available rules and their status.

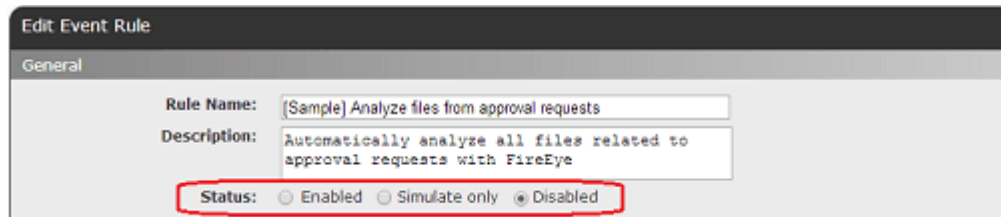


2. Check the box next to one or more rules in the table.
3. On the Action menu, choose **Enable** or **Disable** and confirm your choice in the confirmation dialog. The checked rules are enabled or disabled according to your menu choice.

If you want to enable or disable a single Event Rule, you can use the Edit Event Rule page. This is also where you can activate *Simulate only* mode, which allows you to see what the effect of an event rule would be without having it take the action specified in its definition.

**To enable, disable or simulate the effect of an Event Rule:**

1. On the console menu, choose **Rules > Event Rules**. The Event Rules page appears, showing the available rules and their status.
2. Click the View Details button next to the rule whose status you want to change. The Edit Event Rule page opens.



3. In the Status field, click the radio button for **Enable**, **Simulate Only** or **Disable**.
4. Make any other changes to the rule properties and click **Save** to stay on the page to monitor events processed by the rule or **Save & Exit** to leave the page. See [“Testing a Rule before Enabling”](#) on page 427 for a sample workflow for *Simulate only* rules.

**Note**

If an event rule depends on a particular configuration of an analysis tool, such as an analysis environment with a specific operating system, and if that environment becomes unavailable, the rule will be disabled automatically after waiting several minutes for the environment to become available again.

**To delete event rules in the Event Rules table:**

1. On the console menu, choose **Rules > Event Rules**. The Event Rules page appears, showing the available rules and their status.
2. Check the box next to one or more rules in the table.
3. On the Action menu, choose **Delete** and confirm your choice in the dialog. The checked rules are deleted.

## Disabling Processing of All Event Rules

By default, the Bit9 Server is configured to process any enabled event rules. This means that the Enabled/Disabled/Simulate setting for each rule determines how and whether that rule functions. However, you can disable the event rule feature so that no event rules are processed. The checkbox for disabling and re-enabling event rule processing is on the

Advanced Options tab of the System Configuration page. When you disable event rules, any alerts based on event rules will not be triggered.



#### To disable all event rule processing:

1. On the console menu, choose **Administration > System Configuration** and click on the **Advanced Options** tab.
2. Click the **Edit** button at the bottom of page.
3. In the Software Rule Options panel, *un-check* the Event Rules checkbox, then click the **Update** button.

To re-enable event rules, follow the same steps, except check the Event Rules box. Re-enabling event rules causes them to continue processing each rule from the point it was stopped. This can be useful when infrastructure activities would prevent event rules from completing their actions. For example, if you had many analysis rules that required access to a connected appliance and the appliance was down for maintenance, you could disable rule processing until the maintenance is completed.

## Testing a Rule before Enabling

Event rule actions, such as bans, approvals and moving computers between policies, can cause serious security and operational issues if not properly configured. Because of this, it is strongly recommended that any new rule be run in *Simulate only* mode before it is fully enabled – this is one of the options on the Add and Edit Event Rule pages.

When you run an event rule in Simulate only mode, you can apply the rule to past notifications and view the events that *would have been* processed by the rule. You can then review these results, and you may choose to add or change filters for the rule to reduce the conditions under which the rule is triggered. If you open the Edit Event Rule pages for the sample rules, you can see some of the ways filters have been used to limit events processed by the rule. “[Sample Event Rules](#)” on page 438 describes these rules.

#### To test the effects of a rule with Simulate only mode:

1. On the console menu, choose **Rules > Event Rules**. The Event rules page appears, showing the available rules and their status.
2. Click on the View Details button next to the rule you want to test. The Edit Event Rule page for that rule opens.
3. Examine the configuration of the rule, changing it if necessary.
4. In the Status field, check the **Simulate only** radio button.
5. Make any other needed changes to the rule and click the **Save** button  
**Note:** You must remain on the Event Rule details page to complete this process, so do not click the *Create & Exit* button.
6. On the Advanced menu to the right of the page, click on **Re-apply rule** choose a time period in the dialog box. This determines the window of past events the rule will be applied to. Depending upon the volume of matching events, you might want to limit the initial test to a short period, such as **1 day**. Choose the time period and click **Go**.

7. Continue to monitor the page, periodically clicking **Refresh Page** in the Processed Events panel until the Last Processed Event field in the History panel shows no more events to process. See “[Event Rule History and Processed Events List](#)” on page 437 for an example of the information shown in the Processed Events panel.
8. If you don’t see events you expected to appear in the Processed Events panel, or if you see more or different events than expected, modify the rule accordingly, click **Save** again, and reapply the rule. Events related to the rule should appear in the table of events with a *Simulated* in the Status field.
9. To simulate the rule for a longer period, change the *Re-apply rule* value and click **Go**.
10. Once you see events you expect and determine that the rule has no negative effects, change rule Status to **Enabled** and click **Save & Exit**. The rule is executed on new events – use the *Re-apply* menu if you want the rule to run actively on past events.

## Creating and Editing Event Rules

You can create a new event rule by copying and modifying the settings of an existing rule or by creating the rule from scratch. In either case, you would need to provide at least the non-optional information shown in bold in the left column:

General Description	Section in the Add/Edit Event Rule Page
If a <b>file-related event matches this/these criteria</b> ...	Select Event Properties
...and a <b>file referenced in the event matches this/these criteria</b> (optional)...	Select File Properties
...and the <b>process referenced in the event matches this/these criteria</b> (optional)...	Select Process Properties
... then <b>take the following action</b> ...	Select Action
... on computers in <b>this/these policy(ies)</b> ...	Select Action/Create For:

The Select Event Properties, Select File Properties, and Select Process Properties sections can include multiple criteria for triggering the rule, and the Select Action section has different parameters depending on the action you choose.



**To add (create) an event rule:**

1. On the Bit9 console menu, choose **Rules > Event Rules**. The Event Rules page opens.
2. On the Event Rules page, choose **Create Rule**. The Create Event Rule page opens. [Table 62, “Event Rule Parameters”](#), on page 431 describes the settings on this page.

3. If there is an existing event rule similar to the one you want to create, choose that rule on the Copy Settings From menu. When you choose anything but (none) on this menu, the page is pre-populated with the parameters from the rule you chose, and you need only change the parameters that differ from the rule you copied from.
4. In the Rule Name field, provide a unique name for the rule. If you copied settings from an existing rule, the default name is that rule’s name followed by “(Copy)”.
5. In the Description field, you can provide a longer description of the rule if you choose. (Completing this field is optional).
6. In the Status field, you choose one of the following:
  - **Enabled** – Actions specified by the rule will be executed as specified.
  - **Simulate only** – Actions specified by the rule will be simulated. Events will be generated indicating what the rule would have done if enabled, but the actions specified will not actually be taken.
  - **Disabled** – The rule and its settings will be saved but it will not execute or simulate the actions specified.

**Important:** *Simulate only* is strongly advised as the choice for a new event rule. See [“Testing a Rule before Enabling”](#) on page 427 for more about this Status choice.

7. In the Select Event Properties panel, use the Add filter menu to choose one or more event properties. For these filters:
  - At least one Subtype filter must be included.
  - Because only file or computer-related events may be used to trigger an event rule, the selections on this menu are limited accordingly.
  - Some file-related properties that appear in events are not included here because they appear on the File Properties menu.
  - To use file names or path names in an event rule filter, you should specify them using the Event Properties filter rather than File Properties filter. The Event Property *File name* usually matches more of the relevant events than the File Property *First seen name*.
8. In the Select File Properties panel, use the Add filter menu to choose one or more file properties with which to further refine the conditions under which this rule will be triggered. Most of the choices here are the same as the fields in the Bit9 File Catalog, although there are some additional fields. See [“File and Process Properties in Event Rule Definitions”](#) for detailed information about certain choices in this panel.

#### Note

For both Select File Properties and Select Process Properties, if you choose an Extension filter, you must use the file extension *without* the initial dot (for example, *bat*, not *.bat*). Otherwise the rule will not function properly.

9. In the Select Process Properties panel, use the Add filter menu to choose one or more process properties with which to further refine the conditions under which this rule will be triggered. Most of the choices here are the same as the fields in the Bit9 File Catalog, although there are some additional fields. See [“File and Process Properties in Event Rule Definitions”](#) for detailed information about certain choices in this panel.

**Note:** The process to which this configuration choice applies is the *parent process* of the file referenced in the event or event rule, not the process that appears in the operating system task manager when a file executes.

10. In the Select Action panel, use the Action menu to choose the action that will be taken when events and files match this rule. The options that appear on this menu depend upon the permissions of the console user creating or editing the rule – see [“Account Group Permissions”](#) on page 93. The possible choices are:
  - **Change global file state** – This automatically changes the global state of matching files. You can Approve or create a Report Only Ban for matching files, or Remove Approvals or Bans. You also can apply the state change to All policies or selected policies.

**Note:** The setting that creates an actual (not a Report Only) ban via an event rule is disabled by default. Contact Bit9 Support if you want to activate this feature.
  - **Change local file state** – This automatically changes the local state of matching files. You can locally Approve matching files or Remove local approval.
  - **Upload file** - This initiates an upload to the Bit9 Server of matching files from the Bit9-managed computer on which they appear. You can choose the default upload location or define a custom location on the server or another accessible computer.

For example, you can send all newly found files to a specific folder for manual examination or scanning by a tool that exists on a particular system.

**Note:** *Manage uploads of inventoried files* which is required for this action, is not a default permission for any standard account groups.

- **Analyze file** – This initiates the process for sending a file to a connected device for analysis. You can choose any analysis service you have configured with the Bit9 Connector, and can send the file to more than one service.
- **Move computer** – This moves the computer referenced in the event to a different policy when an event matching the rule occurs.

**Note:** The Move computer option is disabled by default. Contact Bit9 Technical Support if you want to use this feature.

11. If the choice on the Action menu involves changing the state of a file, you can choose to have any approval request related to the file resolved automatically. To do this, check the **Resolve Related Approval Request** box. If you do not check the box, any approval request for the related file will be left open until you manually close it. This box has no effect if there is not a related approval request. See [“Approval Requests and Justifications”](#) on page 467 for more on how approval requests are submitted and resolved.
12. When you have completed the rule definition, click **Save** to remain on the page, and follow the steps described in [“Enabling, Disabling, and Deleting Event Rules”](#).  
-or-  
To create the rule and leave the Create Event Rule page, click **Create & Exit**.

[Table 62](#) shows the parameters available on the Create/Edit Event Rule page.

**Table 62:** Event Rule Parameters

Panel:Field	Description
<b>Copy Settings From:</b>	Existing rule from which this rule should copy its initial settings. If you do not want to copy any settings, leave the default value of (none).
<b>Rule Name</b>	Name by which this rule is identified. (Required)
<b>Description</b>	Additional information about the rule. This can be any text you choose to enter. (Optional)
<b>Status</b>	Radio buttons that determine whether and how this rule is activated: <ul style="list-style-type: none"> <li>• <b>Enabled</b> – Actions specified by the rule will be executed as specified.</li> <li>• <b>Simulate only</b> – Actions specified by the rule will be simulated. Events will be generated indicating what the rule would have done if enabled, but the actions specified will not actually be taken. This is the default value for newly created rules.</li> <li>• <b>Disabled</b> – The rule and its settings will be saved but it will not execute or simulate the actions specified. This is the default value for the sample rules.</li> </ul>

Panel:Field	Description
<b>Select Event Properties: Add Filter</b>	<p>The properties of the event that triggers this rule:</p> <ul style="list-style-type: none"> <li>• <b>Subtype</b> – At least one event Subtype filter must be included in this filter (For example, <i>New file on network</i>). Additional Subtypes may be added so that, for example, a rule is triggered for either <i>New file on network</i> or <i>New unapproved file to computer</i> events.</li> <li>• <b>Other Event properties</b> – Other properties may be added to this filter. Some file-related properties that appear in events are not included here because they appear on the File Properties menu.</li> </ul>
<b>Select File Properties: Add Filter</b>	<p>File properties with which to further refine the conditions under which this rule will be triggered. Most of the choices here are the same as the fields in the Bit9 File Catalog, although there are some additional fields. See <a href="#">“File and Process Properties in Event Rule Definitions”</a> on page 435 for detailed information about certain choices in this panel. File properties are not required in an Event Rule.</p> <p><b>Note:</b> If you specify a file property and that property is unavailable, the rule cannot be executed, and events matching the rule are placed in a Pending state until the property becomes available. For example, if you specify that the an event rule requires that the Bit9 SRS reputation for a file shows that it has a Trust level of 5 or less, if Bit9 SRS is not configured and there is no trust information for the file, the rule will not be executed, even if all other rule parameters are met. This also applies to file prevalence and metadata.</p>
<b>Select Process Properties: Add Filter</b>	<p>Process properties with which to further refine the conditions under which this rule will be triggered.</p> <p>Most of the choices here are the same as the fields in the Bit9 File Catalog, although there are some additional fields. See <a href="#">“File and Process Properties in Event Rule Definitions”</a> on page 435 for detailed information about certain choices in this panel. Process properties are not required in an Event Rule.</p> <p><b>Note:</b> If you specify a process property and that property is unavailable, the rule cannot be executed, and events matching the rule are placed in a Pending state until the property becomes available. For example, if you specify that an event rule requires that the Bit9 SRS reputation for a file shows that it has a Trust level of 5 or less, if Bit9 SRS is not configured and there is no trust information for the file, the rule will not be executed, even if all other rule parameters are met. This also applies to process file prevalence and metadata.</p>

Panel:Field	Description
<b>Select Action:</b> <b>Action</b>	<p>The following options appear on the Action menu:</p> <ul style="list-style-type: none"> <li>• <b>Change global file state</b> – This automatically changes the global state of matching files. You can Approve or create a Report Only Ban for matching files, or Remove Approvals or Bans. You also can apply the state change to All policies or selected policies.  <b>Note:</b> The ability to initiate an actual (as opposed to Report Only) ban using an event rule is disabled by default. Contact Bit9 Support if you want to activate this feature.</li> <li>• <b>Change global process state</b> – This automatically changes the global file state of matching processes. You can Approve or create a Report Only Ban for matching processes, or Remove Approvals or Bans. You also can apply the state change to All policies or selected policies.</li> <li>• <b>Change local file state</b> – This automatically changes the local state of matching files. You can locally Approve matching files or Remove local approval.</li> <li>• <b>Upload file</b> - This initiates an upload to the Bit9 Server of matching files from the Bit9-managed computer on which they appear. You can choose the default upload location or a custom location on the server or another accessible computer. For example, you can send all newly found files to a specific folder for manual examination or scanning by a tool that exists on a different computer.  <b>Note:</b> This option is available only for console users with one or both <i>Manage uploads of inventoried files</i> permission. See <a href="#">“Account Group Permissions”</a> on page 93.</li> <li>• <b>Analyze file</b> – This initiates the process for sending a file to a connected device for analysis when the rule conditions are met. You check the box for one or more enabled analysis services integrated with the Bit9 Server through the Bit9 Connector. If no services are configured, this option does not appear.</li> <li>• <b>Move computer</b> – This moves the computer referenced in the event to a different policy, with the following options: <ul style="list-style-type: none"> <li><b>Specify policy</b> – This displays a menu of the policies available on this Bit9 Server.</li> <li><b>Restore to normal enforcement level</b> – This returns a computer that is in Local Approval mode to its previous policy. If the computer is not in Local Approval mode, this has no effect.</li> <li><b>Local approval</b> – This moves a computer into Local Approval mode. See <a href="#">“Moving Computers to Local Approval Mode”</a> on page 258 for details.</li> <li><b>Automatic policy</b> – This moves a computer into the policy to which Active Directory mapping assigns it. If AD Mapping is not enabled, this setting has no effect.</li> </ul> <b>Note:</b> The <b>Move computer</b> option is disabled by default. Contact Bit9 Support if you want to use this action. </li> </ul>
<b>Resolve Related Approval Request</b>	<p>When the Action choice for the rule is Change Global file state or Change local file state, this checkbox is displayed. If the box is checked, any approval request related to the file referenced in this file has its status changed to Resolved.</p>
<b>Priority</b>	<p>When the Action choice for a rule is Upload file or Analyze file, you can set the priority for the upload or analysis to Low, Medium, or High, which determines the order in which the action is taken relative to other upload or analyze requests. Priority can be changed on the Requested Files page once a request is in progress.</p>

## Editing an Event Rule

You can edit existing event rules, modifying the parameters described in [Table 62, “Event Rule Parameters”](#) on page 431. However, you cannot change the Action setting for a rule once it is created; different actions may require different Bit9 Console user account permission, and also, rule history might not make sense if the rule recorded a mix of different actions. If you need to change the Action, create a new rule. You can use the *Copy Settings from* field to copy most of an existing rule parameters and then change the action before saving. Note also that you can change some of the options underneath an Action (such as changing which policies it applies to or changing Approval Request settings).

### Edit Event Rule Page Menus

The Edit Event Rule page has two menus on the right side of the page. The Related Views menu has one or more of the following commands (which vary depending upon the Action chosen for the rule):

- **All file rules created by this rule** – Displays the Software Rules: Files Approvals and Bans page filtered to show file rules created by this event rule (does not include local file approvals, which are not tracked on this page)
- **All file uploads created by this rule** – Displays the Requested Files: Uploaded Files page filtered to show uploads initiated by this rule
- **All file analysis submissions created by this rule**-- Displays the Requested Files: Analyzed Files page filtered to show analysis submissions to analysis services configured through the Bit9 Connector
- **Related events** – Displays the Events page, filtered by this rule name

The Action menu includes one or more of the following commands:

- **Cancel all file analysis submissions created by this rule** – For file analysis rules, cancels all unprocessed file submissions made to analysis services configured through the Bit9 Connector. This has no effect if a file submitted because of this rule has already been sent to the analysis service.
- **Cancel all file uploads created by this rule** – For file upload rules, cancels all unprocessed file uploads initiated by the rule. This has no effect if a file has already been uploaded.
- **Create Alert** – This opens the Add Alert page and partially configures the alert with information from the event rule. If completed and saved, the alert reports each time this event rule is triggered.

The Advanced menu includes one or more of the following commands:

- **Re-apply rule** – This allows you to choose a starting point in the past and re-apply this rule to all events that occurred between that point and the current time. This is useful for testing new or edited rules in *Simulate only* mode before switching to *Enabled* mode. It also can be used to re-apply rules to older events after switching to enabled mode.
- **Clear processed events** – This clears Simulated, Executed, and Skipped events in the Processed Events panel. Pending events are not cleared.

## Event Rule Ranking

Event Rules are processed in the order of the rank, with the highest ranked (lowest numbered) rule processed first. Processing order does not depend on the current sorting order of the table, only on the rank number of the rule. All matching rules that are currently enabled are processed. You can sort by rank and then use the up and down arrows next to each rule on the Event Rule page to change the rank of the rules.

## File and Process Properties in Event Rule Definitions

Certain choices in the Select File Properties and Select Process Properties panels of the Add/Edit Event Rule page have special behaviors affecting how they are evaluated. A common issue is what happens when an event occurs that is missing data specified in an event rule filter. Evaluation of that event is put into a Pending state until the data becomes available. The following sections describe this and other behaviors that may affect rule evaluation.

### Bit9 SRS Trust and Threat Data

If you choose one of the Bit9 SRS parameters, *Trust* or *Threat*, in the File or Process Properties for a rule, only events that have a value for these fields will trigger the rule. Events whose files do not have a Trust or Threat value will go into Pending state (visible in the Processed Events list for the rule) until Bit9 SRS information is available. Once data becomes available, the event will be evaluated against the rule.

Another behavior to be aware of is the treatment of Trust values that are unknown but not missing. If Bit9 SRS and Bit9 Server have synchronized file information and there is no trust information for a file, no Trust value is shown in the Bit9 Console. However, the *stored* Trust value for a file whose trust is unknown is minus one (-1). Therefore, an event rule that specifies that an action should be taken for files with less than a certain trust will be triggered for both low trust files *and files whose trust is unknown*. To limit the rule action to files for which the trust is known to be low (as opposed to unknown), add a second condition that specifies Trust must also be greater than or equal to zero.

### File Prevalence

If you choose file *Prevalence* as a filter parameter, only events for which prevalence is calculated for a related file will trigger the rule. Events whose files have no prevalence value will go into Pending state until a Prevalence value is available. Also, keep in mind that certain settings will make it impossible to accurately report prevalence, including exclusion of Microsoft Support file tracking and exclusion of tracking in selected policies.

### File Metadata

If any file metadata field (such as file type, file size, company, publisher, and product) is used as part of a file or process filter, an incoming event will be evaluated only after the specified metadata is reported for that particular file by the agent. The delay between when an event is reported and when the related file message arrives should be on the order of seconds. However, if an agent has a large backlog of files to report or goes offline just after sending an event, the delay could be long enough to place event rule evaluation into the Pending state.



## File Extension

For both Select File Properties and Select Process Properties, if you choose file Extension as a filter, you must use the file extension *without* the initial dot. For example, to specify that a rule is triggered for batch files with the *bat* extension, you would use *bat* alone, not *.bat* (dot bat). Otherwise the rule would not function properly.

## Analysis Results Options

The Select File Properties and Select Process Properties filter menus include file analysis options that are not available in the Bit9 File Catalog. These options can be used to take action based on the results of analysis by external devices. The options are *Analysis Result: Check Point*, *Analysis Result: Palo Alto Networks Wildfire*, *Analysis Result: FireEye*, and *Analysis Result: Microsoft SCEP*, each of which shows the latest analysis results for a file from their respective devices. These choices can have one of the following values:

- **Unknown** – The file was not yet analyzed by this service.
- **Clean** – The file was analyzed with this provider and nothing suspicious was found.
- **Potential Risk** – The file was analyzed with this provider and a potential risk was detected. Note that this state can currently only be set only by FireEye, when user creates a matching Threat Mapping.
- **Malicious** – The file was analyzed with this provider and is reported as malicious.
- **Analysis Pending** – The file is still being analyzed with this provider.
- **Analysis Error** – The file was analyzed but analysis returned an error.

As with the Bit9 SRS and Prevalence filters, rules with analysis filters will go into the Pending state for an event that matches the rule but for which analysis results are not available.

### Note

For FireEye notifications, if you created Threat Mapping rules, review these rules before creating event rules. Threat mapping might change the values provided for analysis results and so change the conditions under which an event rule is triggered. See [“FireEye Threat Level Mapping”](#) on page 715.

## Global Bans for Non-Cataloged Files

You can use an Event Rule to create a global ban for a file that has not yet been seen on a Bit9 Agent reporting to your server. This would happen if you specified a certain event subtype, such as Malicious file detected, in the Event Properties for the rule, and then an analysis service connected to the Bit9 Server reported a file that triggered an event matching the rule definition. If no other properties are defined for the rule, it immediately creates a “pre-ban” for the file so that if it does appear on any of the agent computers, it will already be banned.

However, if a File Properties filter is added to the rule definition, the rule goes into the Pending state until the reported file actually appears on an agent-managed computer and can be evaluated against the specified properties. If a Process Properties filter is defined and an event has no process associated with it, the event will be silently skipped, leaving no record in the event view.



## How Event Rule Approvals Affect Endpoints

Local approvals initiated by an event rule happen immediately (or as soon as an agent connects to the server). However, unlike most other approvals, event rule global or by-policy approvals are not pushed to endpoints automatically. Like Reputation Rules, Event Rules have three conditions that cause a file approval to be sent to endpoints:

- If the Bit9 Server has a record of a file being blocked *on any endpoint* and that file is later approved by event rule, the server begins sending the approvals of the file to connected agents immediately.
- If a user attempts to execute an instance of an event-rule-approved file on a computer connected to the Bit9 Server, the server will allow the agent to run the file immediately, and also will begin sending the approval to other agents.
- If an event-rule-approved file is identified as an installer, the Bit9 Server begins sending the approval of the file to agents immediately.

Even if a file is approved by event rule and not blocked by another rule, until its approval is sent to agents because of one of the conditions above, instances of the file may be locally unapproved and may block if the agent computer is disconnected from the server before the approval is distributed.

If a file was approved globally or by-policy using an event rule and then an event rule removes that approval, the approval for that file is eliminated for connected computers, and the file state in the File Catalog reverts to unapproved. However, if an instance of this file was executed during the time it was approved by event rule, all instances on computers connected at that time remain *locally approved*.

## Event Rule History and Processed Events List

A history of the events processed by each rule is included in the History panel on the Event Rule Details (Edit Event Rule) page. This history is automatically trimmed as events are trimmed from your Bit9 database.

The screenshot shows the 'History' panel for an event rule. It displays metadata such as 'Date Created', 'Created By', 'Date Modified', 'Last Modified By', 'Last Evaluation Time', and 'Last Processed Event'. Below this are buttons for 'Save & Exit', 'Save', and 'Cancel'. The 'Processed Events (603)' section is expanded, showing a table of events with columns for Date Executed, Status, Timestamp, Type, Subtype, and Source.

Date Executed	Status	Timestamp	Type	Subtype	Source
May 21 2013 03:15:55PM	Simulated	May 21 2013 03:15:01PM	Discovery	New file on network	MYCORP\Laptop-1
May 21 2013 03:09:52PM	Simulated	May 21 2013 03:09:16PM	Discovery	New file on network	MYCORP\Laptop-7
May 21 2013 03:09:52PM	Simulated	May 21 2013 03:09:16PM	Discovery	New file on network	MYCORP\Desktop-5
May 21 2013 03:07:52PM	Simulated	May 21 2013 03:06:58PM	Discovery	New file on network	MYCORP\Laptop-9
May 21 2013 03:05:51PM	Simulated	May 21 2013 03:05:39PM	Discovery	New file on network	MYCORP\Desktop-4
May 21 2013 03:04:50PM	Simulated	May 21 2013 03:04:01PM	Discovery	New file on network	MYCORP\Desktop-4

The History includes the following information:

- **Date Created** – The time stamp for when this rule was created.
- **Created By** – The Bit9 Console login account of the user who created the rule.
- **Date Modified** – The time stamp for when the rule was last modified.
- **Last Modified By** – The Bit9 Console login account of the user who last modified the rule.
- **Last Evaluation Time** – The time stamp of the last time the rule was triggered by a matching event. In addition, this field shows statistics for any activations of the rule in the past hour, including the number of times it was triggered, the number of events processed, and the time elapsed for processing.
- **Last Processed Event** – The time stamp of the last event that was processed with this rule. This value can be useful in determining whether there is a significant backlog in processing events and also to determine events in the event log that might be processed next. Note that “processing” means the *rule* was processed, not that the resulting *action* has been completed.

Below the History panel, the Event Rule Details page shows a table of Processed Events that have been processed by the current rule. This can help you monitor the impact of a rule. The table shows the Status of each processed event, which is one of the following:

- **Pending** – The event matched the rule but the rule action has not been completed. If information is available about why the action is in this state, it is displayed as a tooltip when you hover over the Status.
- **Simulated** – The event was processed by the rule in Simulate only mode; the processing was recorded but the action was not executed. See [“Enabling, Disabling, and Deleting Event Rules”](#) for more information.
- **Executed** – The event was processed by the rule and the specified action was executed.
- **Skipped** – The rule was skipped because it would have taken an action that is prohibited or not relevant to the current conditions. For example, a rule cannot globally approve a banned file.

## Sample Event Rules

The Event Rules page, which you access by choosing **Rules > Event Rules** on the Bit9 Console menu, includes several sample rules. You can click on the View Details button to open the Event Rule Details page for any of these rules to see how they were specified. You also can use them (or any other existing rule) as a template for a new rule. For example, you could modify a rule to ban or analyze files and processes referenced when an event with *Carbon Black watchlist* subtype is reported.

### Note

If an event rule depends on a particular configuration of an analysis tool, such as an analysis environment with a specific operating system, and if that environment becomes unavailable, the rule will be disabled automatically after waiting several minutes for the environment to become available again.

## Sample Rule: Analyze files from approval requests

This rule sends any file for which an approval request is made to one or more analysis services. By default, it sends files to WildFire, but you can change the rule to send files to any of the analysis services you have configured through the Bit9 Connector tab on the System Administration page, and can require a result from more than one service. Files that have already been reported by the services you choose are not sent for analysis. See “[Approval Requests and Justifications](#)” on page 467 for more information about approval requests and [Chapter , “Bit9 Connector for Network Security Devices,”](#) for more information about using Bit9 Connector to integrate analysis services with the Bit9 Platform.

The default properties of this rule are:

- **Event Properties:** Subtype is *Approval request created*
- **File Properties:** Analysis Result: Palo Alto Networks WildFire is *Unknown*
- **Process Properties:** None
- **Action:** Analyze file
  - **Priority:** Medium
  - (Analysis Service Choice): Unchecked

## Sample Rule: Resolve approval requests for clean files

This rule performs two actions on files submitted in approval requests if they have been analyzed with WildFire and found to be Clean: it locally approves them, and it resolves the related approval request. If used, it should be enabled along with the *Analyze files from approval requests* rule and ranked after it, so that files are analyzed before their approval requests are resolved.

The default properties of this rule are:

- **Event Properties:** Subtype is *Approval request created*
- **File Properties:** Analysis Result: Palo Alto Networks WildFire is *Clean*
- **Process Properties:** None
- **Action:** Change local file state
  - **Change local state:** Approve
  - **Resolve Related Approval Request:** Unchecked

The rule can be modified to take action based on analysis results from multiple connected devices or services; it will be Pending until all of analysis requests have completed.

## Sample Rule: Analyze downloaded files

This rule submits certain files downloaded to a Bit9-managed computer from a web browser to Palo Alto Networks WildFire for analysis. It excludes files with properties that suggest they should be trusted or that have already been reported by or do not meet the requirements for WildFire analysis. It also excludes partially downloaded files.

The default properties of this rule are:

- **Event Properties:**
  - **Subtype** is *New file on network*
  - **Process** ends with *iexplore.exe* or *firefox.exe* or *chrome.exe*.
  - **File Name** doesn't contain *.crdownload* or *.part*
- **File Properties:**
  - **File Size** smaller than *10240000*
  - **File State** is not *Approved*
  - **File Type** is *Application*
  - **Analysis Result: Palo Alto Networks WildFire** is *Unknown*
- **Process Properties:** None
- **Action:** Analyze file
  - **Priority:** Medium
  - (Analysis Service Choice): Unchecked

## Sample Rule: Report malicious files

This rule applies a global Report Only ban to all malicious files detected by Bit9 SRS or any of the appliances or services integrated with Bit9 as part of the Bit9 Connector.

The default properties of this rule are:

- **Event Properties:** Subtype is *Malicious file detected*.
- **File Properties:** None
- **Process Properties:** None
- **Action:** Change global file state
  - **Change Global State:** Ban (Report only)
  - **Resolve Related Approval Request:** Unchecked
  - **Create for:** All policies

Because this is a Report only rule, it is not necessary to test this in Simulate only mode first.

## Chapter 17

# Block Notifiers and Approval Requests

This chapter describes the notifiers that appear on agent-managed computers when a Bit9 rule blocks file access or related actions. It describes how notifiers are assigned to different rules, standard notifier behavior, options available to the user for responding to a notifier, ways to customize notifiers, and how to enable and use the Bit9 approval request management feature.

### Sections

Topic	Page
<a href="#">Notifiers: What Users See</a>	442
<a href="#">The Bit9 Console Notifiers Page</a>	447
<a href="#">Assigning Notifiers to Settings and Rules</a>	447
<a href="#">Customizing and Creating Notifiers</a>	450
<a href="#">Notifiers in Windows Session Virtualization</a>	464
<a href="#">Approval Requests and Justifications</a>	467

## Notifiers: What Users See

The Bit9 Agent runs silently in the background until it detects and blocks an action for which there is a blocking rule. When the agent blocks an action, it can display a *notifier* on the computer where the action was attempted, notifying the user of why the action was blocked. Depending upon the blocked action and the configuration choices made on the Bit9 Server, notifiers can also give the user options for responding to the block.

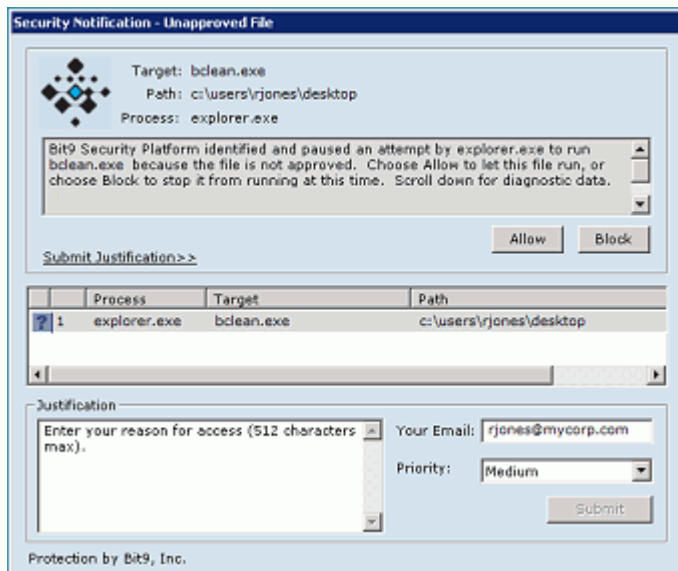
All of the descriptions below assume that notifiers are enabled for all rules and settings.

### Note

Notifiers are supported for Windows 8 and Windows 8 Pro in version 7.2.1, but only when these systems run in traditional desktop mode. Notifiers are not supported in the Metro interface.

## Prompt Notifiers

*Prompt* notifiers tell the user what the attempted action was and why it was interrupted, but also give the user the option of allowing or blocking the action.

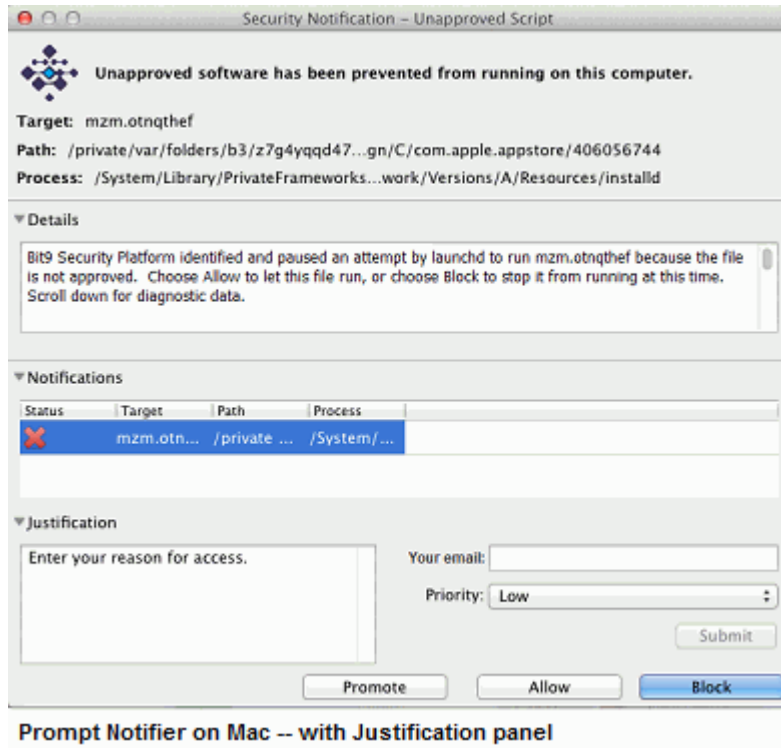


Users see Prompt notifiers under these conditions:

- When they attempt to execute an Unapproved file on a computer that is in Medium (Prompt Unapproved) Enforcement Level.
- When they attempt an action that is governed by a Custom (File and Path) Rule, Registry Rule, or Memory Rule, and that rule is configured to prompt for a decision.

Because they require a response from the user, Prompt notifiers cannot be disabled in custom, registry or memory rule definition, and they *should not* be disabled for any policy setting that defines a rule that could prompt the user.

If the Justification option, which is part of the Approval Request feature, is enabled, users can send a *justification* of the choice they make in responding to the notifier. This should be done *before* choosing to allow or block the action. See [“Approval Requests and Justifications”](#) on page 467 for more information about this feature.



The choices on a prompt notifier depend upon the conditions that caused the block:

- **Block** leaves the action blocked, makes no changes in the state of files or devices, and dismisses the notifier.
- **Allow** lets the action take place. If it was a blocked execution of an Unapproved file because of Medium Enforcement on the computer, the file is locally approved and allowed to run, and if it is recognized as an installer, files written by it are locally approved. If it is not recognized as an installer, files it writes are not locally approved.
- When an action is blocked by a file execution rule, holding down the Shift key activates the **Promote** button in Mac and Linux and replaces **Allow** with **Promote** in Windows. Promote ensures that the file runs as a promoted process, meaning that files written by the process will be locally approved. This is useful if the notifier is displayed for an execution attempt on a file that installs other files but is not recognized by Bit9 as an installer.
- If the user takes no action on a prompt notifier after 10 minutes, the file is blocked, a block event is recorded on the Bit9 Server, and the notifier is dismissed. However, any interaction with the dialog (e.g., clicking on it or moving it) will prevent the timeout.

## Block-only Notifiers

*Block-only* notifiers inform the user that their action was blocked and why, but do not give the user the option of allowing the action. Users see block-only notifiers, if enabled, under these conditions:

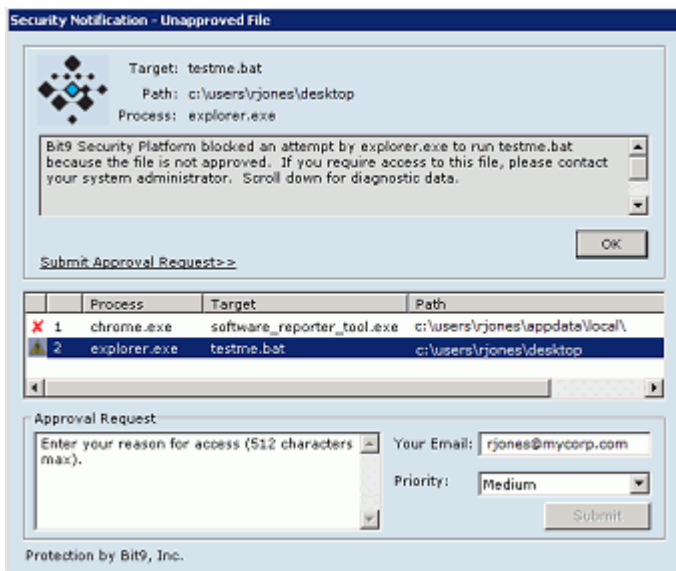
- When they attempt to execute a banned file on a computer that is in Control mode.
- When they attempt to execute an unapproved file on a computer that is in High (Block Unapproved) Enforcement Level.

- When they attempt an action that is governed by a Custom Rule, Registry Rule, or Memory Rule, and that rule is configured to block the action.
- When they attempt a file action on a device that is governed by a Device Rule that blocks the action.

The appearance and options a block-only notifier depends on the platform on which the notifier appears.

## Block Notifiers on Windows Computers

On Windows computers, block notifiers appear as full-sized dialogs. There is no option for taking action on the blocked file or device. Users dismiss the notifier by clicking **OK** or using the **Esc** key.



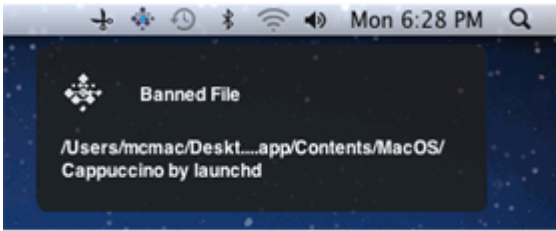
If the Approval Request feature is enabled, users can send formal requests for access to files or devices that they can't currently access. Approval Requests are enabled by default in new Bit9 installations beginning with v7.0.0. See [“Approval Requests and Justifications”](#) on page 467 for more about this feature, including details about enabling approval requests if you are upgrading from a previous release.

Block-only notifiers can be disabled without disabling their underlying rules.

## Block Notifiers on Mac and Linux Computers

On Mac (OS X) and Linux computers, block notifiers appear as a small, translucent notification panel with information about the operation and action that was blocked. Because the notification does not require action, this panel will fade and disappear in five seconds unless the user clicks on it. If a new block happens while this notifier is displayed, the new block resets the timer to five seconds.





Clicking on the block notifier before it fades opens the Bit9 Notifier history window, which provides a history of notifier events that have occurred on the computer. See [“Bit9 Notifier Tray Icon and History Window”](#) on page 446 for details about the information and actions available on the notifier history window.

## Notifier Components

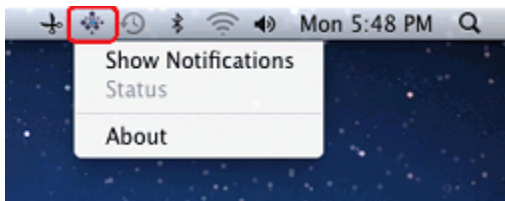
Full-sized notifiers (all Windows notifiers and Prompt notifiers on Mac and Linux) can include the following components, some of which are always shown, some of which are optional, and some of which can be customized:

- The title appears at the top of the window. For example, “Security Notification – Unapproved File”.
- The notifier provides information about the Target of the action (e.g., the file the user attempted to execute), its path, and the process that attempted to execute it.
- A logo appears in the upper left of the notifier to help identify the source of the block. By default, this is the Bit9 logo. The logo also can be eliminated.
- On Mac and Linux computers, an additional subtitle appears, for example “Unapproved software has been prevented from running on this computer.”
- Notifier text, which appears in the top-most text box in the notifier, provides a description of what was blocked and why. For example, “Bit9 blocked an attempt by explorer.exe to run calc.exe because the file is not approved. If you require access to this file, please contact your system administrator.” On Mac and Linux computers, similar detail is available for each notifier event in the Bit9 Notifier history window – see [“Bit9 Notifier Tray Icon and History Window”](#) on page 446.
- On Windows computers, the optional notifier link provides a link to a URL, which can point to a site that explains security policy and/or provide an opportunity to request access to a blocked object. It also can be configured to initiate a mail message to request access.
- On Windows computers, a history panel in the notifier itself shows the files that have been blocked on this computer. A green checkmark indicates that a file was allowed to run or write. A red ‘x’ indicates that the file or action was blocked, either by a Bit9 rule or by the user’s choice. A yellow triangle indicates that the notifier timed out before the user took action (and so the action was blocked). A question mark indicates the current block event (i.e., the one that caused the current notifier to display). On Linux and Mac, a similar history is available in the Bit9 Notifier history window – see [“Bit9 Notifier Tray Icon and History Window”](#) on page 446.
- An Approval Request or Justification panel allows users to file formal approval requests for files or devices that they can’t currently access, or justifications for why they chose to allow an action if they were given a choice in the notifier. See [“Approval Requests and Justifications”](#) on page 467 for more about this feature.

## Bit9 Notifier Tray Icon and History Window

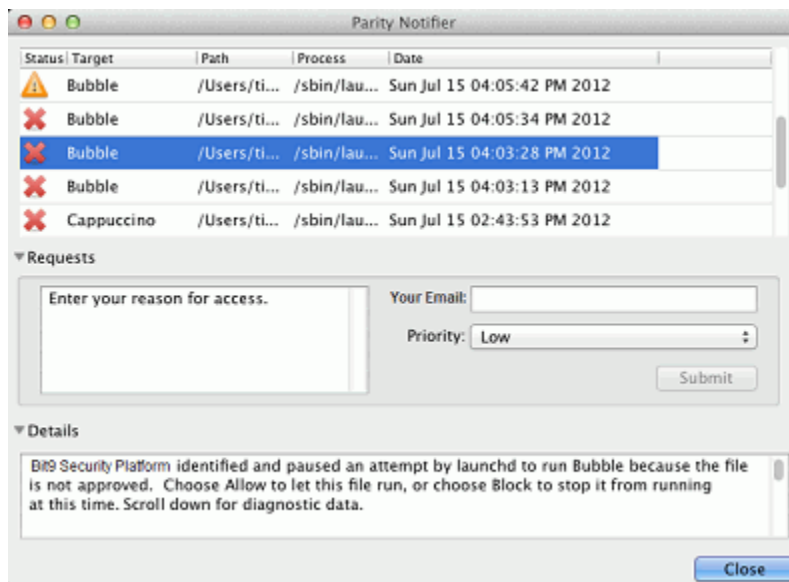
On Linux and Mac computers, installation of the Bit9 Agent adds a tray or panel icon that can be used to access a menu with the following options:

- **Show Notifications** – This opens the Bit9 Notifier history window, which shows past blocks events and the notifier information associated with them. It also provides access to the interface for submitting approval requests for previously blocked files.
- **About** – This shows the Bit9 Agent version and copyright information.



### Bit9 Notifier History Window

On Linux and Mac computers, the Bit9 Notifier history window shows past blocks events. If the user selects a block event, they can get details about it and submit a request for the blocked file or action to be approved.



On Windows computers, each notifier includes a history panel that functions much the same way as the history list in the Mac or Linux notifier. The key difference is that in Windows, the history is available only when a notifier is displayed – there is no separately accessible Bit9 Notifier history window.

The list of block events includes the following information:

- **Status** – This is indicated by an icon: a red X for blocked files or actions; a green check for files or actions that were allowed because of user choice on the notifier; a yellow triangle if the notifier timed out before the user took action (and so the action was blocked).
- **Path** – The full path to the file that was blocked.

- **Process** – The full path to the process that attempted the action.
- **Date** – The date and time the file or action was blocked.

Below the history list, the Requests panel allows the user to request approval of the blocked file selected in the list. This panel can be shown and hidden by clicking on the arrow next to its name.

Below the Requests panel, the Details panel provides a more detailed description of the file or action that was blocked. This panel can be shown and hidden by clicking on the arrow next to its name.

## The Bit9 Console Notifiers Page

Notifiers available to Bit9 Agents are shown in a table on the Notifiers page in the Bit9 Console. This page includes the default notifiers provided with the current Bit9 release and any notifiers you have added. In addition, if you upgraded from a previous version of Bit9 (Parity) and modified any of the notifiers, both the 7.2.1 default and the modified version are listed in the Notifiers table. The first modified version of a 6.0.2 notifier has “(custom 1)” appended to the name, the second “(custom 2)”, etc.

You can edit any notifier on the page, but you cannot delete the default notifiers.

Notifier Name	Title	Timeout	Use Count
Block banned file hashes	Security Notification - Banned File	0	4
Block banned file hashes(custom 1)	Security Notification - Banned File	0	1
Block banned file names	Security Notification - Banned File	0	4
Block banned file names(custom 1)	Security Notification - Banned File	0	1
Block banned file names(custom 2)	Security Notification - Banned File	0	1
Block custom path	Security Notification - File and Path Custom Rule	0	1

## Assigning Notifiers to Settings and Rules

Notifiers can be assigned in two places in the Bit9 Console:

- On the Edit Policy page, for each policy setting
- On the Add/Edit Rule page for custom, registry, and memory rules; a rule can be configured to use the notifier assigned by a computer’s policy or to use a custom notifier specified in the rule details

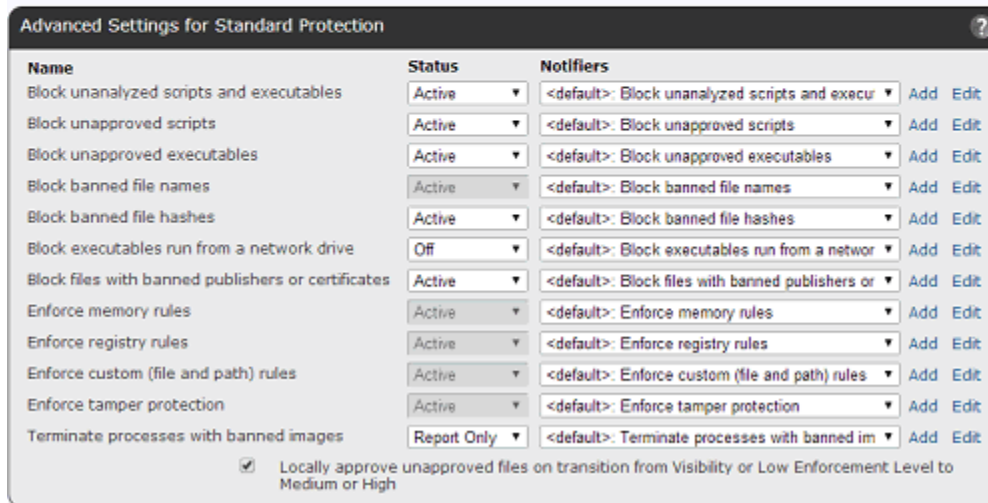
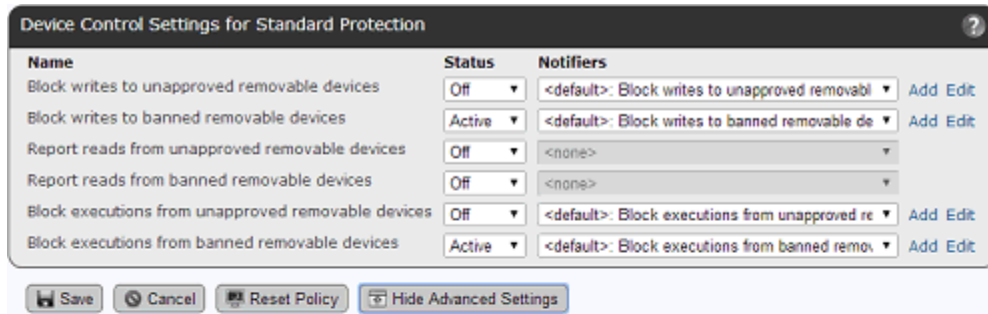
### Assigning Notifiers to Policy Settings

A default, setting-specific notifier is assigned to each policy setting, so notifier configuration is not required. However, you can choose a different notifier from a menu for each rule and setting. This section describes how you assign existing notifiers to

settings. See “Customizing and Creating Notifiers” on page 450 for information about modifying notifiers or creating new ones.

**To assign a notifier to a policy setting:**

1. On the console menu, choose **Rules > Policies**. The Policies page appears.
2. On the Policies page, click the View Details button next to the name of the policy whose notifier assignments you want to change. The Edit Policy page appears.
3. To change the notifier for an Advanced Setting, click **Show Advanced Settings**.]



4. For the setting whose notifier you would like to change, make a new choice from the Notifiers menu.  
You can choose <none> to display no notifier when a setting blocks an action. Consider all conditions for a setting, however, before changing its notifier to <none>. For example, if you choose <none> for *Block unapproved executables*, users in Medium Enforcement policies, who should be able to choose whether to block or allow execution of unapproved files, will not have the opportunity to make that decision. The file will be blocked without any notice from the agent.
5. Click the **Save** button to preserve your changes. The Policies page appears.
6. Repeat steps 3-5 for each setting that you want to change in this policy.
7. Repeat this procedure for each policy whose notifiers you want to change.

## Policy Settings with Notifiers

Each of the following policy settings, which appear in the Device Settings and Advanced Settings lists on the Edit Policy page, has its own separately assigned notifier:

### Device Settings with Notifiers:

- Block writes to unapproved removable devices
- Block writes to banned removable devices
- Block executions from unapproved removable devices
- Block executions from banned removable devices
- Report reads from unapproved devices (will never display notifier)
- Report reads from banned devices (will never display notifier)

### Advanced Settings with Notifiers:

- Block unanalyzed scripts and executables
- Block unapproved scripts
- Block unapproved executables
- Block banned file names
- Block banned file hashes
- Block executables run from a network drive
- Enforce memory rules
- Enforce registry rules
- Enforce custom (file and path) rules
- Enforce tamper protection
- Terminate processes with banned images

## Assigning Notifiers to Custom, Registry and Memory Rules

A notifier can be displayed when a custom, registry, or memory rule blocks an action or prompts the user for a decision to allow or block an action. For each rule, you can choose from two sources for the notifier:

- **Use Policy Specific Notifier** – Each Policy includes an Advanced Setting for each rule type. Each of these policy settings has a Notifier field in which you can specify the notifier that appears on agent computers when that type of rule blocks an action. You also can choose <none> to allow a rule to block an action without displaying any notifier. By default, rules that block or prompt use the policy-specific notifier.
- **Custom Notifier** – If you do not want to use the policy-specific notifier, you can assign any available notifier to any rule. The notifier choices appear on a menu on the Add/Edit page for the rule. You also can Add a new notifier or Edit an existing notifier. See [“Customizing and Creating Notifiers”](#) on page 450 for details.

The screenshot shows the 'Definition' window for a 'File Integrity Control' rule. The 'Rule Type' is 'File Integrity Control'. The 'Write Action' is 'Block', and the 'Custom Write Notifier' is '<none>'. A red box highlights the 'Write Action' and 'Custom Write Notifier' fields. Below these fields are 'Path Or File' and 'Process Exclusion' fields, and a 'Rule Applies To' section with radio buttons for 'All policies' and 'Selected policies'.

When you choose Prompt as the rule action, Custom Notifier menu does not include <none> as an option because a prompt rule requires a notifier to appear.

When you choose Block as the rule action, you can choose <none> on the Notifier menu for a rule since it is possible you want the rule to block actions without notification.

If you choose Use Policy Specific Notifier for a rule, it is possible that the policy specifies <none> as the Notifier for one of its rule types. In this case, a notifier will not be shown, even for a Prompt rule. Unless you are certain that you never want to prompt the user for a response to a rule, choosing <none> for the rule notifier in a policy is not recommended.

## Customizing and Creating Notifiers

You can edit existing notifiers, and you also can create new notifiers. If you edit one of the default notifiers, you can later reset that notifier to its original settings.

The combination of notifier text, notifier link, notifier name, and custom logo path cannot exceed 1900 characters in length. You will see a warning if you exceed the limit.

### To customize an existing notifier:

1. There are three ways to open the Edit Notifier page:
  - On the console menu, choose **Rules > Notifiers**, and in the Notifiers table, click the View Details (file and pencil) button next to the name of the notifier you want to edit.
  - On Device Settings or Advanced Settings panel of the Edit Policy page, click **Edit** in the far right column next to the name of the notifier you want to edit.
  - On the Edit page for a Custom, Registry or Memory rule, if the Custom Notifier menu is showing, click **Edit** next to the name of the notifier.

**Edit Notifier Block banned file hashes**

Name: Block banned file hashes

Notifier Title: Security Notification - Banned File

Notifier Text: <BlockText:Bit9 Security Platform blocked an attempt by <ProcessName> to run <TargetName> because the file is banned. If you require access to this file, please contact your system administrator.> Scroll down for diagnostic data.

Notification Logo: Bit9 Logo

Notifier Link:

Notifier Timeout: 0 seconds (0 = never timeout, -1 = never display)

Approval Request: Approval Request

Policy Name	Rule Name
Template Policy	Block banned file hashes
Maximum Protection	Block banned file hashes
Local Approval Policy	Block banned file hashes
IT Group	Block banned file hashes
Default Policy	Block banned file hashes

Save Cancel Reset Notifier

2. Review and change the notifier settings you want to change (see [Table 63](#)).
3. Click the **Save** button to preserve your changes.

**Table 63:** Add/Edit Notifier Settings

Field	Description
<b>Copy Settings From</b>	(For Add Notifier page only) Existing notifier from which to copy the initial settings for the new notifier. You can use this to populate all of the new notifiers fields and then modify only those you want to change. Choose ( <i>none</i> ) if you want to fill in all notifier fields from scratch.
<b>Name</b>	The notifier name as it will appear in the Notifiers table and menus on the policy and rule pages. This name does not appear on notifier displayed to the computer user.
<b>Notifier Title</b>	Window title for the notifier message that the computer user sees when the agent blocks file execution as a result of this setting.
<b>Notifier Text</b>	Explanatory message displayed in the notifier on Windows computers when the agent blocks file execution as a result of this setting. You can modify this message, tag different messages for block-only vs. block-and-prompt conditions, add tags that provide event-specific information, and add other conditional text. Tags here also can modify the Approval Request feature.  See <a href="#">“Editing Notifier Text”</a> on page 453 for a description of tags. See <a href="#">“Approval Requests and Justifications”</a> on page 467 for a description of how to activate and configure Approval Requests. <b>Platform Note:</b> Notifier Text appears only on Windows notifiers.



Field	Description
<b>Notifier Logo</b>	<p>By default, the Bit9 logo appears in the notifier dialog box when a Bit9 setting blocks a file. The Notifier logo menu gives you these options:</p> <ul style="list-style-type: none"> <li>• Leave <b>Bit9 logo</b> as the selection.</li> <li>• Choose <b>Custom</b> and provide a URL or file path to a different image. See <a href="#">“Specifying a Custom Notifier Logo”</a> on page 460 for details about image format and file path requirements.</li> <li>• Choose <b>None</b> to display no logo or image in the notifier.</li> </ul>
<b>Notifier Link</b>	<p>Either:</p> <ul style="list-style-type: none"> <li>• a link to an informational web page where the computer user can learn more about your security settings and procedures for responding to blocked files, or</li> <li>• a <i>mailto</i>: link to allow the user to send questions by mail</li> </ul> <p>The URL or mailto link provided here can appear literally in the notifier or be represented by a “Friendly Text” description.</p> <p>Leave this field blank if you choose not to display a URL or mailto link at this time.</p> <p><b>Platform Note:</b> For this release, Notifier Links appear only on Windows notifiers.</p>
<b>Notifier Timeout</b>	<p>The number of seconds that a block-only notifier stays on the screen on a Windows computer. After the specified period of time, the notifier is automatically closed.</p> <p>The default timeout value is zero (0), which leaves the notifier on screen so that the user must respond to it. A value of negative one (-1) instructs agents not to display the notifier at all. See <a href="#">“Disabling Bit9 Notifiers”</a> on page 463 for additional information about enabling and disabling blocked action notifiers.</p> <p><b>Platform Note:</b> This value affects Windows computers only. On Mac and Linux, a block-only notifier times out in 5 seconds by default.</p>
<b>Approval Request</b>	<p>Determines whether and how the Approval Request feature is enabled for this notifier. The choices are:</p> <ul style="list-style-type: none"> <li>• <b>None</b> - No approval request panel is displayed.</li> <li>• <b>Approval Request</b> - The Approval Request panel appears when a rule completely blocks access to a file.</li> <li>• <b>Justification</b> - The Justification panel appears when a rule prompts a user to allow or block an action.</li> <li>• <b>Approval Request and Justification</b> - The Approval Request/Justification panel appears for both block and prompt conditions.</li> </ul> <p>See <a href="#">“Approval Requests and Justifications”</a> on page 467 for more details.</p>
<b>Notifier Applies to</b>	<p>(Appears only if the notifier is assigned to at least one setting or rule) This panel lists all of the rules and settings to which the notifier is assigned. You can remove all of these assignments by clicking <b>Remove Associations</b> in the Advanced menu. If you do this, the affected policy settings revert to their default notifier and the affected rules revert to the policy-specific notifier for their rule type.</p>



The illustration below shows where some of the changes in the Add/Edit Notifier dialog affect the notifier content.



## Creating a New Notifier

Creating a new notifier is similar to editing an existing notifier, with the exception of the initial steps.

### To add (create) a new notifier:

- There are three ways to open the Add Notifier page:
  - On the console menu, choose **Rules > Notifiers**, and in the Notifiers table, click **Add Notifier** button.
  - On Device Settings or Advanced Settings panel of the Edit Policy page, click **Add** in the far right column next to the name of the notifier you want to edit.
  - On the Edit page for a Custom, Registry or Memory rule, if the Custom Notifier menu is showing, click **Add** next to the name of the notifier.
- If you want to start with the settings of an existing notifier, choose a notifier from the Copy Settings From menu.
- Enter or edit settings as necessary (see [Table 63](#)).
- Click the **Save** button to preserve your changes.

**Note:** Once you click Save on the Add Notifier page, the notifier is saved and added to the Notifiers list. If you navigated to the Add Notifier page from a policy, the new notifier is saved even if you did not click Save on the Edit Policy page.

## Editing Notifier Text

You can customize the notifier text a user sees when a Bit9 rule blocks an action. For example, you might want to add a description of the “Promote” option to the notifiers for your existing policies, unless you prefer not to highlight this option. The Bit9 Notifier supports conditional, meta and reporting tags that can be used to tailor the information reported to the end user.

**Platform Note:** Notifier text appears on the Prompt notifier for all platforms, on the Block-only notifier for Windows, and on the Bit9 Notifier history dialog for a selected item in the history. Notifier messages also appear in the Windows event log.

## Using Tags in Notifier Text

Notifier text and links can include tags that provide information specific to the event that caused the notification, such as the name of the computer the event occurred on and the policy in force at the time. [Table 64](#) shows the informational tags you can add to a notifier message – note that you might see other tags that are for Bit9 support purposes only.

### Notes

In addition to providing conditional information to the user, tags in the notifier text box can be used to customize the Bit9 Approval Request feature. See [“Approval Requests and Justifications”](#) on page 467 for more information about these tags and how to use them.

**Table 64:** Informational Notifier Tags

Tag	Description	Example Values
<ComputerName>	The local name of the computer on which the block event occurred	“RJONES-LAPTOP”
<DebugInfo>	Technical information about the rule and policy that generated the event. This is a metatag (that is, it contains information represented by other tags)	
<DomainName>	The NetBIOS domain name of the computer on which the block event occurred	“MYCORP”
<EnforcementLevel>	The Enforcement Level of the agent at the time the block occurred	“High (Block Unapproved)”, “Medium (Prompt Unapproved)”, “Low (Monitor Unapproved)”
<Operation>	The type of operation that was blocked	“Execute”, “Write”, “Read”, etc.
<OsVersion>	The version, build and release of Windows on the agent computer	“Microsoft Windows 7 x64 (build 7600)”
<Bit9AgentVersion>	The version of the agent running on the system on which the operation was blocked.	“7.2.1.256 (Patch 3)”
<Policy>	The policy the agent computer is in	“Research Team”, “Sales Group”, “Guests”, etc.
<ProcessName>	The name (without the path) of the process that was blocked	“explorer.exe”
<ProcessPath>	The path (without the name) of the process that was blocked	“c:\windows\system32\”

Tag	Description	Example Values
<ProcessPathName>	The full path, including name, of the process that was blocked	"c:\windows\system32\explorer.exe"
<ProcessPublisher>	The publisher name for the source process, if signed	"Bit9, Inc", "Google Inc.", "Microsoft Corporation", etc.
<ProcessSha256>	The SHA256 hash (hexadecimal) of the source process	
<RuleType>	The type of rule that was triggered	"File and Path", "Registry", "Memory", "Process", etc.
<TargetName>	The name (without the path) of the target file, registry key or process name to which access was attempted	"foo.bat"
<TargetPath>	The path of the target file, key or process (without the name)	"c:\test\"
<TargetPathName>	The full path and name of the target	"c:\test\foo.bat"
<TargetPublisher>	The publisher name for the target file, if signed	"Bit9, Inc", "Google Inc.", "Microsoft Corporation", etc.
<TargetDevice>	The drive letter of the device on which an action was blocked. Unmapped devices are shown as \\device\ <i>&lt;name&gt;</i> .	
<TargetShare>	The network path (without the filename) to the remote drive on which access to a file was blocked.	"\\SERVER3\temp\mydir"
<TargetSha256>	The SHA256 hash (hexadecimal) of the target file	
<TargetSha1>	The SHA1 hash (hexadecimal) of the target file	
<TargetMD5>	The MD5 hash (hexadecimal) of the target file	
<UserName>	The name of the user in whose context the blocked operation was initiated	"\MYCORP\rjones"

## Conditional Messages for Block vs. Prompt

By using conditional tags within the same notifier text, you can show the user one message for block-only notifiers, when an action is simply blocked by a Bit9 rule, and a different message for prompt notifiers, when a user is asked whether to block or permit an action. For example, you can create a single notifier text block that displays a "block" message to a user in a High Enforcement Level policy who attempts to execute an

unapproved file, but displays an “ask” message to a user in a Medium Enforcement Level policy if they attempt to execute the same file. Similar prompt messages can be used for custom, registry or memory rules in which the user is offered the option of blocking or allowing an action. [Table 65](#) shows the tags for different block conditions (“*message*” represents the variable text you use in the message).

**Table 65:** Conditional Notifier Tags

	Description
<BlockText: <i>message</i> >	Text to display if the rule blocks an action and the user has no choice to allow it.
<AskText: <i>message</i> >	Text to display if the rule prompts the user for a decision on whether to block or proceed with an action. This is the most generic “prompt” case.
<AskAllowText: <i>message</i> >	Text to display if the rule prompts the user for a decision on whether to <i>block or allow file execution</i> .
<AskRestrictText: <i>message</i> >	Text to display if the rule prompts the user for a decision on whether to <i>allow or restrict memory access</i> .
<AskApproveText: <i>message</i> >	Text to display if the rule prompts the user for a decision on whether to <i>block writing of a file or to approve the file and allow it to be written</i> .

For example, when an unapproved file is blocked, the notifier text might include the following:

```
An unapproved file attempted to run on this
computer<BlockText: and has been blocked. If you require
access to this file, please contact your system
administrator.><AskText:. Choose Allow to continue to let
this file run, or choose Block to prevent it from running at
this time.>
```

When a computer with an agent in a High enforcement policy with this notifier text attempts to execute an unapproved file, the notifier message uses the *BlockText*:

```
An unapproved file attempted to run on this computer and has
been blocked. If you require access to this file, please
contact your system administrator.
```

However, when a computer with an agent in a Medium enforcement policy with this same notifier text attempts to open an unapproved file, the notifier message uses the *AskText*:

```
An unapproved file attempted to run on this computer. Choose
Allow to continue to let this file run, or choose Block to
prevent it from running at this time.
```

You can nest other tags inside the conditional block/ask tags shown in [Table 65](#). For example, the following is the default notifier message for *blocked*, *unapproved* files:

```
<BlockText:Bit9 blocked an attempt by <ProcessName> to run
<TargetName> because the file is not approved.  If you
require access to this file, please contact your system
administrator.><AskText:Bit9 identified and paused an
attempt by <ProcessName> to run <TargetName> because the
file is not approved.  Choose Allow to let this file run, or
choose Block to stop it from running at this time.>
```

Notice that there are other tags nested inside both the BlockText and AskText conditional tags. The conditional block/ask tags are the only notifier *text* tags inside which you can nest other tags. In the notifier *link*, you can nest tags inside the “FriendlyText” tag.

### Note

When you upgrade Bit9 Server from a previous release, your existing notifier messages are preserved, including those for Default and Template policies. Especially if you began with a pre-6.0.2 version of Bit9 (Parity), your notifiers might not include conditional text to provide different messages for “block” conditions and “ask” conditions and other special tags.

## Informational Tags as Conditional Operators

In addition to the special “block-and-ask” conditional operators, notifier messages can include other conditional text based on any of the informational tags shown in [Table 64](#), except for the metatags, such as <DebugInfo>. You construct conditional text tags as follows:

```
<tagnameText:pattern-to-match:message-text>
```

You must append the word “Text” directly to the end of the tag name: the tag will not work without this addition.

For example, to set up notifier text that appears only if the computer on which an action is attempted is running Bit9 Agent 7.0.0, you would use the <Bit9AgentVersion> tag as shown in the following example:

```
<Bit9AgentVersionText:7.0.0.*:This will display only on
7.0.0 agents>
```

Note that the asterisk wildcard character in “7.0.0.\*” is used so that any build number of Bit9 Agent 7.0.0 matches the condition. The asterisk matches zero or more of any character; the question mark matches any one character (but not zero characters).

As another example, you could set up notifier text to appear if the hash for a target file matches a particular SHA-256 hash, using the <TargetSha256> tag. You could nest this

conditional text within a generic “file blocked” notifier, as shown in the following example:

```
Bit9 blocked an attempt by <ProcessName> to run <TargetName>
because the file is banned.
<TargetSha256Text:c1c4eacd1fe39c93df477f335644902b3b83cc437b
fe4b641960f874af1e0708:This version of MyFavoriteApp has a
major security flaw.>
If you require a solution to this block, please contact your
system administrator. Scroll down for diagnostic data.

<DebugInfo>
```

## Editing the Notifier Link

A notifier link is the link your users can click on when an action is blocked to contact your inhouse support desk or go to a web page that explains more about why the action was blocked. Although you can use the same notifier link for all conditions in which Bit9 blocks a file action, you have the option of providing a different link for each notifier, and as with notifier text, you can embed tags to provide more information about the event in the link.

A notifier link is one method for managing requests for access to a file or device, and may be a good choice if you already have IT policies in place for collecting and responding to these requests. Bit9 also provides its own Approval Request feature, which populates the notifier with the fields necessary for the user to compose and submit a request and manages these requests directly on the Bit9 Console. See [“Approval Requests and Justifications”](#) on page 467 for more information.

**Platform Note:** Notifier links display only on Windows notifiers.

## Tags in Notifier Links

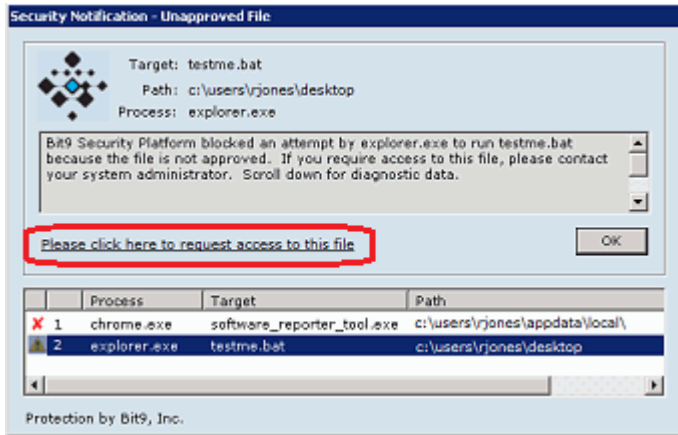
In the **Notifier link** field of the Add/Edit Notifier page, there are two ways in which you can take advantage of notifier tags:

- You can use tags to customize notifier mail messages or site URLs. This can be helpful for creating automated work-flow requests or making a website link automatically go to information about the file that caused the notifier to appear. [Table 64, “Informational Notifier Tags,”](#) on page 454 shows the complete list of these tags.
- You can create “FriendlyText” to display on the notifier dialog in place of the URL itself. The FriendlyText tag may appear anywhere in the notifier link text.

The following notifier link demonstrates both of these uses of tags:

```
mailto:it@mycorp.com?subject=Request approval of
<TargetName>&body=<UserName> on
<DomainName>\<ComputerName>has requested access to
<TargetName>.%0AFile details available at https://
bit9server1/file-details.php?hash=<TargetSha256>
<FriendlyText:Please click here to request access to this
file.>
```

When the notifier text above is used in the “Block unapproved executables” notifier, if an agent computer in a High Enforcement policy attempts to execute an unapproved file, a notifier is displayed similar to the following:



Notice that instead of displaying the notifier link URL (“mailto:mycorp.com...”), the link shows the “Friendly Text” (“Please click here...”), which provides an indication of why they would click on the link.

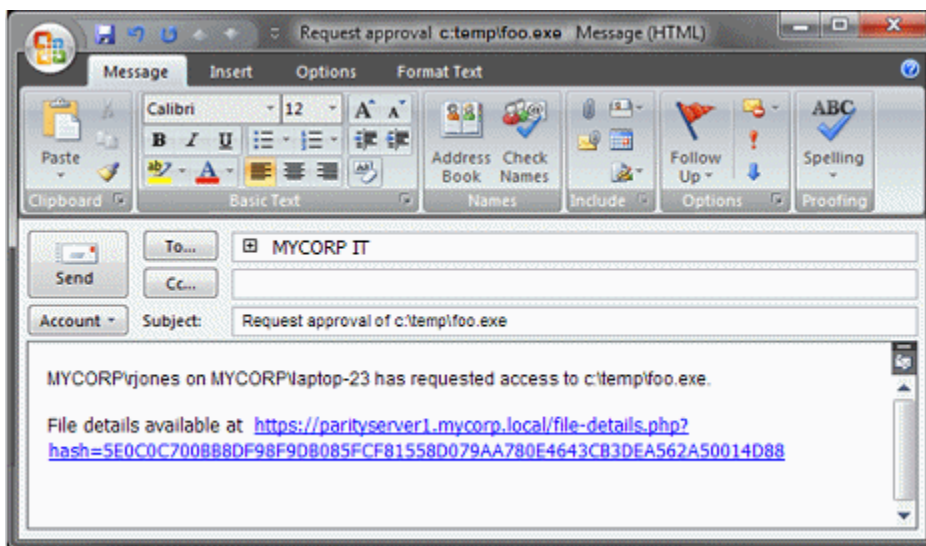
You can nest other tags inside a FriendlyText tag. For example, instead of the generic link text shown above, you could create the following link:

```
<FriendlyText>Please click here to request access to
<TargetName>.>
```

which would insert the name of the file that was blocked in the link text.

Whether you display a URL or friendly text, the resulting link text is displayed as one or two lines. The text will not interfere with the action buttons (“OK”, “Allow”, “Block”), and if link text is too long, it is truncated to fit on the dialog box.

In the example shown, when the user clicks on the link, a mail message similar to the following is initiated in the user’s default mail client:



The notifier link defined above used tags to make several customizations:

- It generated an email message to the organization’s IT group requesting access to an unapproved file.
- It specified the name of the file in the message header.
- It identified the user, the computer, and the file in the message body.
- It provided a URL in the mail message that points directly to the File Details page in the Bit9 Console for the specific file in the request.

If this were a “block-and-ask” situation in which the end user could make his or her own judgment about a file, you could create a simpler notifier link that goes directly to the URL for the file details (without generating a mail message), similar to the following:

```
https://bit9server1/file-details.php?hash=<TargetSha256>  
<FriendlyText:Please click here for information about this  
file.>
```

## Editing the Notifier Source Line

There is a line at the bottom of notifiers that identifies the source of the notifier. By default, this says *Protection by Bit9, Inc.* You can change this line by inserting the following tag into the Notifier Text field, substituting your own source identification for *text*:

```
<NotifierComment:text>
```

If you want to eliminate this line from the notifier, use a single space as your *text*.

**Platform Note:** The Notifier Source line displays only on Windows notifiers.

## Specifying a Custom Notifier Logo

By default the notifier that is displayed when files are blocked on an agent computer includes the Bit9 logo. You also have the option of having no logo on a notifier, or of providing a custom logo. Logos are specified on a per-notifier basis.

### Important

- Pre-7.0.0 implementations of a custom logo, including both special solutions provided by Bit9 Technical Support and the standard customization available in Bit9 (Parity) 6.0.2, are not maintained when you upgrade to v7.2.1. You must use the method below to implement custom logos. If you specified a custom logo in v7.0.0 or later, that will be maintained on upgrade.
- Pre-6.0.2 Bit9 Agents will not display a newly configured custom logo until they are upgraded.



**To specify a custom logo for a notifier:**

1. On the console menu, choose **Rules > Notifiers**. The Notifiers page appears.
2. On the Notifiers page, either:
  - Click **Add Notifier** if you are creating a new notifier. The Add Notifier page appears.
  - or-
  - Click the View Details (file and pencil) button next to the name of an existing notifier you want to edit. The Edit Notifier page appears:

The screenshot shows the 'Edit Notifier Block banned file hashes' dialog box. The 'Notification Logo' dropdown menu is highlighted with a red box and currently shows 'Bit9 Logo'. Other fields include Name: 'Block banned file hashes', Notifier Title: 'Special Banned File Notifier', Notifier Text: '<BlockText:Bit9 Security Platform blocked an attempt by <ProcessName> to run <TargetName> because the file is banned. If you require access to this file, please contact your system administrator.> Scroll down for diagnostic data.', Notifier Link: (empty), Notifier Timeout: '0' seconds, and Approval Request: 'Approval Request'.

3. On the Notifier Logo menu, choose **Custom**. A text box appears next to the menu.

The screenshot shows the 'Notifier Logo' section of the dialog box. The dropdown menu is set to 'Custom' and the text box next to it contains the file path 'c:\logo\mycorplogo.bmp'.

4. Put the file containing the logo you want to use in an accessible location, and enter that location in the Notifier logo text box. You have three options for specifying the location of the logo file:
  - **UNC:** You can provide a network-based path specification to the logo file in the form **\\server\share\path\imagefile.gif**. The Bit9 Agent will attempt to make a local copy. If the file cannot be downloaded, the agent will continue to use the prior image (e.g., the default Bit9 image) until the new image can be obtained. The agent will continue to attempt to download the image once per hour until the image is successfully downloaded or the image is explicitly changed or disabled. **Note:** The **LocalSystem** account must have access to the UNC path you provide for the image to be accessible on agent computers. Also, you must not put the logo in a location that would require a password for access.
  - **URL:** You can specify a web-based path in the form **http://path/imagefile.gif**. This path should be accessible to the Bit9 Agent process and allow anonymous, unauthenticated access. The Bit9 Agent will make a local copy of this file as described above.
  - **Local:** You can specify a local file path (on the local computer) in the form **d:\path\imagefile.gif**. The target file must be locally accessible to the Bit9 Agent process. You must put the logo file on each agent computer that will use it. Any updates to this file take place the next time the notifier is displayed. If the specified path is not accessible, the Bit9 logo is displayed instead and an event is generated once per Bit9 Agent session, just as with non-local paths.
5. Click **Save**. Your changes are saved and the Notifiers page appears.

6. Repeat the steps above for each notifier that should display the custom logo.

## Image File Requirements

Windows systems on which the Bit9 Agent is installed include a blank sample notifier image called **GenericLogo.gif**, which is located in the Bit9 data directory (by default, **ProgramData\Bit9\Parity Agent\images**). Assuming that the agent is installed on the Bit9 Server, you can go to this folder on the server and use GenericLogo.gif as a starting point for creating your own logo image. Otherwise you can copy it from another system that has the agent installed.

The custom image you provide should meet the following requirements:

- The image size should be 60 x 60 pixels.
- The file format should be GIF, JPG or BMP.
- The image should use the same background as GenericLogo.gif; you *cannot* use a transparent background.

## Logo-Related Events

If all Bit9 Agents successfully retrieve your custom logo, there will be no logo-related events generated. If an agent fails to retrieve its logo file, however, an event of subtype “Agent Error” will be generated, noting the computer name and the image file name. If (and only if) there was a failure to retrieve the logo, another event is generated if the computer later successfully retrieves the custom logo.

## Changing the Logo Image

When you specify a non-local image as the notifier logo (i.e., using a UNC or URL path), that image is copied to each agent system, including the server if it has the agent installed. If you change the non-local image but do not change its name, Bit9 Agents will not update to the changed image.

To update the logo image for a notifier, change the name of the image file and update the Notifier logo path for that policy. For example, if you deploy a custom logo **\\server\share\mylogo.gif** and you then modify the logo, you could rename the file to **mynewlogo.gif** and edit the path in the notifier details to **\\server\share\mynewlogo.gif**. Agents in that policy would then update to the new image.

Image files downloaded to agents are not updated or deleted. Because of this, if you switched from mylogo.gif to mynewlogo.gif, and then you switched back to mylogo.gif, the originally downloaded version of mylogo.gif would be used, even if you had modified the source image file.

## Suppressing the Notifier Logo in a Policy

You can prevent display of the notifier logo for all notifiers in a policy. The Suppress Logo in Notifier checkbox on the Add/Edit Policy page suppresses the logo, regardless of what the notifier configuration in each notifier specifies.

## Resetting a Notifier to Initial Settings

You can reset any default notifier to its initial settings. If you do this, you will lose all of the customizations you may have made to this notifier – there is no undo. You reset a notifier by opening the Edit Notifier page for the notifier and clicking **Reset Notifier**. If

there is no Reset Notifier button on the page, the notifier was not one of the default notifiers.

## Resetting a Policy to Initial Notifiers

The Edit Policy page includes a *Reset Policy* button. When you press this button and choose **OK** on the confirmation dialog, the Device and Advanced settings are reset to the *initial* settings of the Template Policy (i.e., the settings in effect immediately after you installed the Bit9 Server). The policy reverts to the default notifiers for each setting.

## Disabling Bit9 Notifiers

There might be situations in which you want to disable notifiers for some or all of your agent computers. For example, if you are running single-purpose devices in High Enforcement, you might simply want to block unauthorized actions without feedback. Block-only notifiers can be disabled without disabling the rules that would otherwise display them. You can disable notifiers on a per setting basis in each policy. You also can disable notifiers for specific custom, memory, or registry rules.

You can disable notifiers only for *block-only* rules. Rules that *prompt* users for a response should always display a notifier.

Disabling Bit9 notifiers does not necessarily mean that actions will be blocked silently. Some Bit9 blocks cause the display of operating system notifiers. Also, events continue to be recorded for blocks even though the notifier is disabled, unless the block is due to a custom, registry, or memory rule that has *Block Silently* as its action.

### To disable notification for a setting in a policy:

1. Open the Edit Policy page for a policy whose notifiers you want to disable.
2. If you want to disable an Advanced Setting notifier, click **Show Advanced Settings**.
3. For the setting whose notifier you would like to disable, choose <none> on the Notifiers menu.  
Consider all conditions for a setting before setting its notifier to <none>. For example, if you choose <none> for *Block unapproved executables*, users in Medium Enforcement policies, who should be able to choose whether to block or allow execution of unapproved files, will not have the opportunity to make that decision. The file will be blocked without any notice from Bit9.
4. Click the **Save** button to preserve your changes. The Policies page appears.
5. Repeat steps 3-5 for each setting that you want to change in this policy.
6. Repeat this procedure for each policy whose notifiers you want to change.

### To disable notification for a specific custom, registry, or memory rule:

1. On the console menu, choose **Rules > Software Rules**.
2. On the Software Rules page, click the tab for the rule type you want to modify.
3. In the table of rules, click the View Details (pencil and file) button next to the rule whose notifier you want to disable.

4. On the Edit Rule page, *un-check* the Use Policy Specific Notifier box next to any actions configured in the rule.
5. In the Custom Notifier menu, choose <none>. Note that <none> is not an option for rules that prompt the user.
6. Click **Save** to preserve your changes.

For Block actions, events are still recorded even if the notifier is disabled. For some rules, you can choose Block Silently from the action menu to disable both notifiers and event recording.

#### **Note**

You also can disable a notifier everywhere it appears (rather than giving a setting no notifier). You do this by entering minus one (-1) as the value for Notifier Timeout on the Add/Edit Notifier page.

## **Notifiers in Windows Session Virtualization**

The Bit9 Security Platform supports special treatment of notifiers for hosted session virtualization environments, such as those provided by Citrix XenApp, Windows Server Remote Desktop Services, and Windows Server Terminal Services. In these environments, you can add special notifier tags that instruct your Bit9 Server to route notifiers in the following ways: If one user is logged into multiple sessions and attempts an action that triggers a notifier, the notifier is displayed to all logged in sessions for that user. For a prompt notifier, responding to any of those notifiers dismisses all of them. For a block notifier, the notifier must be dismissed in each session.

- If multiple users are logged in to one session each, and if one of them attempts an action that triggers a notifier, the notifier is displayed only to the user that triggered the block.
- If an action that triggers a notifier is initiated by the system and not a specific user, you can choose to display the notifier to a specified user or group, all users, or no users. No matter which option you configure, Bit9 logs a block event on the Events page.

- Even when you enable the special notifier behavior, users of agent-managed computers not using session virtualization see notifiers according to the normal rules.

### Notes

- Special treatment of notifiers applies only to *hosted sessions* on a terminal or application server (session virtualization). That is, they apply to a single system and users and applications on that system. Application virtualization that runs applications locally is not compatible with the feature.
- Notifications are always directed to the session of the user taking the action that blocks, not necessarily the originating session. For example, if user A has access to user B's command prompt, and User A executes `runas /user:A cmd.exe` and then executes an unapproved file, the notifier is displayed in user A's remote session, not in the session where user A appeared to have executed the unapproved file.
- **Platform Note:** Broadcast notifiers are available for Windows sessions only.

There are two tags that activate session virtualization notifier behavior:

- **<NotifierBroadcastMessage>** is required to enable special notifier routing. If present, notifiers are displayed on all sessions for the user that initiated an action, or for System actions, as specified by `NotifierBroadcastSystem`.
- **<NotifierBroadcastSystem:user|group|blank>** is used to determine what is done when a system-initiated action is blocked by a Bit9 rule. The default is **<NotifierBroadcastSystem>** with no other arguments. If you leave this tag out but have **<NotifierBroadcastMessage>** in the notifier, notifiers will be displayed to all logged in session users.

The following procedure assumes you want to modify notifier behavior for all settings in a policy. You can add the tags to individual notifiers through the Notifier page if you prefer.

#### To enable special notifier routing for session virtualization:

1. On the console menu, choose **Rules > Policies**.
2. Click on the View Details (pencil and file) button next to the policy whose notifiers you want to edit.
3. Choose a setting whose notifier you want to change and click on the **Edit** button to the right of the Notifier field.
4. In the Edit Notifier dialog, enter **<NotifierBroadcastMessage>** in the Notifier Text field.
5. Also in the Notifier Text field, enter the **<NotifierBroadcastSystem:>** tag with the option you want:
  - To route notifiers for blocks of system-initiated actions to a single user, enter a user name after the colon. For example, **<NotifierBroadcastSystem:MYCORP\jsmith>**

- To route notifiers for blocks of system-initiated actions to members of a group, enter a specified or built-in group name after the colon. For example, **<NotifierBroadcastSystem:MYCORP\itgroup>**
  - To suppress notifiers for blocks of system-initiated actions, do not enter anything after the colon (the colon is optional in this case). For example, **<NotifierBroadcastSystem>**  
Note that if you suppress the notifier in this case, users in Medium Enforcement Level policies will not have the option of allowing unapproved software – it will always be blocked.
  - If you leave the **<NotifierBroadcastSystem>** tag out of the notifier text area but include **<NotifierBroadcastMessage>**, notifiers will be displayed to all logged in session users.
6. **Save** your changes to the notifier.
  7. Repeat for each notifier in the policy (and any others you would like to modify).

## Approval Requests and Justifications

When a Bit9 rule blocks an action, it normally displays a notifier on the computer where the action was blocked. The Approval Request feature allows users to send feedback to administrators when they see a notifier:

- **Approval Requests** – When an action is *blocked* with no option to allow, users might want to request access to the blocked file or device. Bit9 Notifiers can be configured to allow users to submit a formal *approval request* for a blocked file or device.
- **Justifications** – When an action triggers a *prompt* notifier, which provides the user the option to block or allow access, you might want to allow (or require) the user to explain why they allowed the action. The approval request feature also includes an interface for submitting these *justifications*.

When submitted, both approval requests and justifications appear in the Approval Request table in the Bit9 Console, making them easier to manage and respond to. They are recorded in the Bit9 events database. If you choose, you can enable a built-in alert that is triggered when someone makes an approval request. There also is an alert for justifications.

Throughout this chapter “Approval Requests” is the generic term used for the feature that includes both approval requests and justifications. A distinction is made where needed.

Action	Date Requested	Requestor	Reason	Hash	Trust	Threat	Status
<input type="checkbox"/>	Jan 25 2012 03:01:32PM	MYCORP\rijones	I would like to clean my system with this utility.	6AF68...EE3CD	10	0 - Clean	Submitted
<input type="checkbox"/>	Jan 24 2012 03:08:12PM	MYCORP\dbyrd	Banned by accident? Necessary for Java.	6E794...5C69B	10	0 - Clean	Open

### Notes

- Computers running pre-7.0 agents cannot submit approval requests or justifications.
- Approval Requests and justifications are not intended for custom, registry or memory rules.
- As an alternative to the Approval Request feature, you can use *notifier links* as part of an approval request process managed *outside of the Bit9 Console*. Links can be used to automatically open a blank email directed to the person or group responsible for approving files, or they can direct the user to a web page that you use to handle IT requests. See “[Editing Notifier Text](#)” on page 453 for details on setting up these links.  
**Platform Note:** Notifier links appear on Windows computers only.

## Enabling Requests and Justifications

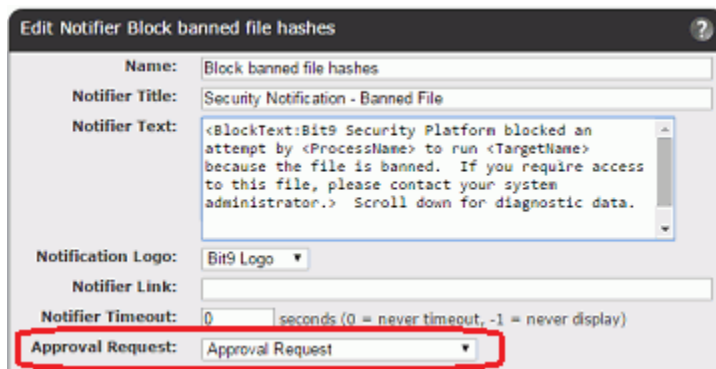
Approval requests and justifications are enabled on a per-notifier basis. What (if anything) you do to enable them depends on whether you are upgrading from a pre-7.0 release, and also on whether you want to customize the appearance and behavior of the feature:

- **New Installations** – In new Bit9 Security Platform installations beginning with version 7.0.0, Approval Requests are enabled for all file and device blocking settings in the Default and Template policies. New policies that you create from these policies will also be configured for approval requests and justifications, and will distinguish between the two in the notifier interface. You should not need to follow the procedure below unless you want to further customize the notifiers.
- **Upgrades** – Upgrades from pre-7.0 versions of Bit9 (Parity) will not have Approval Requests enabled. You can enable them using the Approval Request menu in each notifier, and you can further customize their appearance by adding tags to the notifier text. For upgrades, any notifiers you customized prior to v7.0.1 do not distinguish between *approval requests* and *justifications* in the notifier labelling.

**Platform Note:** Disabling Approval Requests and/or Justifications prevents the related panel from appearing on Prompt notifiers and Windows Block-only notifiers. On Mac and Linux, the Justifications panel is grayed out in the Bit9 Notifier History window when a block event with Approval Requests and/or Justifications disabled is selected.

### To enable Approval Requests and/or Justifications for a notifier:

1. Choose a notifier and open its Edit page.



2. On the Approval Request menu, choose the option you want. The options are:
  - **Approval Request**
  - **Justification**
  - **Approval Request and Justification**
  - **None**
3. Click the **Save** button.

#### Note

You can enable automatic email notification of the requestor when an approval request is closed. See [“Resolving Requests and Justifications”](#) on page 471.

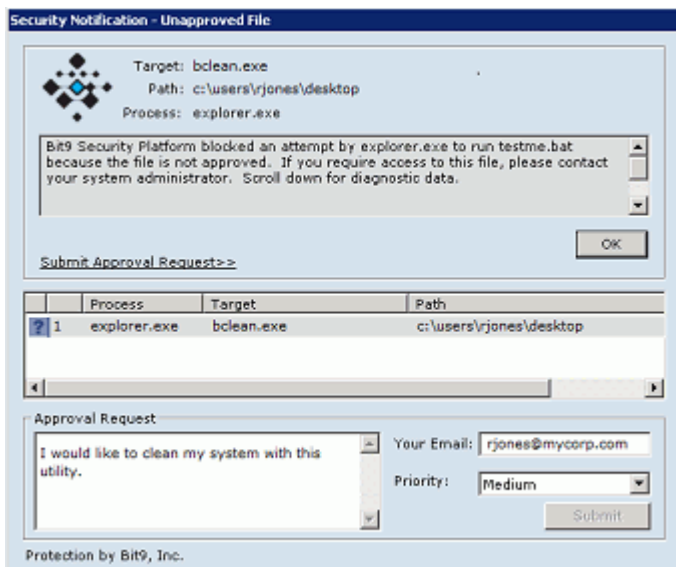


## Submitting Requests and Justifications

When a file action is blocked without an option to allow it, if Approval Requests are enabled, the user can request approval of the file. The location for entering this request varies depending upon the platform.

On Windows computers, Approval Request are submitted through the block notifier. The users can read the notifier's description of the block and why it happened. If the user still wants access to the file or device that was blocked, he or she can type an Approval Request of up to 512 characters into the Approval Request box in the bottom-left section of the notifier. The user has the option of entering an email address if they want that included in the request, and can set a priority, which is Medium by default. Once the text of the approval is entered, the **Submit** button is activated and clicking it submits the request to the Bit9 Server.

On the Windows notifier, the *Submit button*, not the *Submit Approval Request link*, sends the request. The link *Submit Approval Request link* opens and closes the Approval Request panel at the bottom of the notifier.



Submitting a request does not dismiss the Windows notifier. For block-only notifiers, the user still must click **OK** to dismiss the notifier.

On Mac and Linux computers, when an action is completely blocked, users can make approval requests from the Bit9 Notifier history window by selecting any block event from the history and entering the information as described above for Windows (limited to 512 characters). Unlike in Windows, Mac and Linux users can make a series of requests for different file approvals without closing the Bit9 Notifier history.

On all platforms, if a notifier displays a prompt to Allow or Block a file action, the user can submit a *Justification* for choosing to allow a file action. The information is supplied in the same way as for an Approval Request. The user must then click either the **Block** button or one of the buttons that let the action happen (**Allow** or **Promote**).

Once a user submits a request or justification, there is no formal connection to the request from the agent. However, the user can send another request for the same file or device, and can change comments or the priority (for example, if lack of access to a file is preventing them from accomplishing a task) in the resubmission. The response or lack of one is at the discretion of the Bit9 Security Platform administrator reviewing the request.

## Viewing Requests and Justifications

Bit9 Console users with the default Administrator and PowerUser privileges can manage approval requests. In addition, custom groups can be created with permission to view and manage approval requests.

Once submitted, requests and justifications appear on the Approval Request page, which you access by choosing **Tools > Approval Requests** on the Bit9 Console menu. Initially, the request or justification Status is *Submitted* and the Resolution is *Not Resolved*. On the Preferences page (**Tools > Preferences**) you can set the Approval Request page as the Default Starting Page you see on login.

Changing the request Status to *Open* helps indicate that you have begun working on it and is required before you can modify the editable fields in a request. You can Open the request using the Action menu on Approval Requests table page or the Actions menu on the Approval Request Details page.

To see full details for one approval request, you can click on the View Details button (pencil and file) next to a request.

**Approval Request Details**

Request Information

Computer: MYCORP\DESKTOP-8  
Platform: Windows  
Policy: Standard Protection  
Enforcement Level: High (Block Unapproved)  
Request Type: Approval  
Requestor: MYCORP\rjones  
Requestor E-Mail: rjones@mycorp.com  
Priority: Medium  
Rule Type: Unapproved executable  
Reason: I would like to clean my system with this utility.  
Comments:   
Resolution: Not Resolved  
Status: Submitted

Bit9 Platform Analysis

Analysis Not Run Yet.

File Information | Process Information | Installer Information | History

File Name: bcw!pe.exe  
SHA-256: 44bafc75ef0eb3b6784ab8f222e37543f4a4245758425f3b01866ccec4f32bc0  
File State: Unapproved  
Local State: Unapproved  
Publisher: Jetico, Inc. (Unapproved)  
File Prevalence: File exists on 1 computer(s)  
Trust Rating: (unknown)  
Threat Level: (unknown)

Related Views  
[Related File Instances](#)

Actions

On the Approval Request Details page, you can examine details about the request and the requested file or device. You also can edit the request, adding comments and indicating what you did to respond to the request. The Actions menu to the right of the page provides shortcuts to some of the Bit9 rules you might change if you decide to provide access to the blocked file or device.

The Approval Request Details page is divided into the following panels:

- The **Request Information** panel primarily describes the request itself, including the computer and user it came from, and the Bit9 rules and settings relevant to the request. It also includes the user's description of the request, and provides fields for the administrator's response. A complete description of the fields in this panel is available in [Table 66, "Request/Justification Information"](#) on page 476.
- The **Bit9 Analysis** panel is initially blank. If you click the **Run Analysis** button, the panel shows information about the blocked file or device, the user requesting the approval, and other data related to the request. A complete description of the information provided by this analysis is available in [Table 67, "Bit9 Analysis of Requests and Justifications"](#) on page 476. You can click Rerun Analysis to update the information if you've already run it once. This is not a Bit9 Software Reputation Service analysis – you get that by clicking Analyze in the File information tab panel.
- The **File Information** panel shows the name, hash, prevalence, publisher, state, and (if Bit9 SRS is activated and the file is known) trust and threat level of a file that is blocked. You can click the **Analyze** button in this panel to get more Bit9 SRS information about the file. For a description of each field in this panel, see [Table 68, "File Information in Approval Request/Justification Details"](#) on page 478. Note that for device and write blocks of non-executable files, not all information will be available.
- The **Process Information** panel shows information about the process that attempted to initiate the action. For a description of each field in this panel, see [Table 69, "Process and Installer Information in Request/Justification Details"](#) on page 478.
- The **Installer Information** panel shows information about the installer (if known) that installed a blocked file. For a description of each field in this panel, see [Table 69, "Process and Installer Information in Request/Justification Details"](#) on page 478.
- The **History** panel shows any date and time of changes to the approval request, including when it was created, opened, modified and closed. It does not include the history of changes you might make to Bit9 rules in response to the request.

## Resolving Requests and Justifications

When you have reviewed the information in a request or justification and are ready to make a decision about what to do in response, take the following high-level steps:

- Open the request to indicate that you are working on it.
- If you are not rejecting the request, make any needed file state or rule changes.
- Update the status of the request itself and optionally making comments about your decision and actions. This is for auditing purposes and also can be used to provide feedback to the requestor.
- Close the request to indicate that you have finished working on it. If automatic email responses are enabled, this also sends an email to the user that made the request, indicating the decision you made.
- If automatic responses are not enabled and you choose to do so, send mail to the user requesting the approval, indicating the outcome of the request.

**To review and resolve an approval request:**

1. On the console menu, choose **Tools > Approval Requests** and click the View Details button next to the request you want to review. The Approval Request Details page opens.
2. On the Approval Request Details page, choose **Open Request** in the Actions menu or the button at the bottom of the first panel. This activates the Comments, Resolution, and Response E-mail fields.

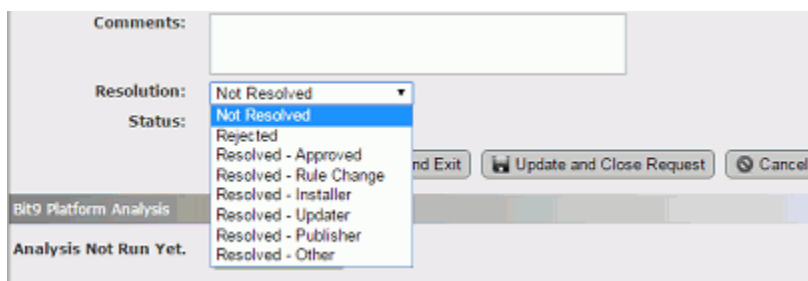


3. If you have chosen to allow access to a blocked file or device, use one of the command shortcuts on the Actions menu to change one or more of the Bit9 rules that caused the block. For example, you might locally approve a file, edit or remove a ban, or globally approve the file.

You are not limited to the commands on the Action menu - it is possible that your response to the request will involve changes to other rules.

**Note:** Any remediation you make does not affect the Resolution or Status fields of the request itself. You must make these changes separately.

4. Indicate what you did (or didn't do) in response to the request by choosing from the Resolution menu in the Approval Request Details. This is for informational purposes only and does not affect file or device state. If you are not allowing access to the requested item, choose **Reject**. Note that the request status must be *Open* for the Resolution menu to be activated.



5. Add or modify the Comments for the request to provide more detail about what you did in response to the request and why.
6. If the Response E-mail address is missing or incorrect and you intend to inform the requestor of the resolution, add or correct the address while the request is still Open.

7. If you are finished working on the request, choose **Close Request** in the Action menu. For multiple requests related to one file, you can choose **Close All Requests for this file**. Closing a request is primarily useful for keeping track of request status, but it also sends request status email to the user that made the request, if automatic email responses are activated.

You can re-open a request if needed.

8. If automatic email notification of requestors is not activated, you can click the Response E-mail address field to open your default email client with a message pre-addressed to the requestor. If you choose to do this, fill in any details you want them to have about your response before sending.

## Notifying Users of Approval Request Resolution

You may choose to notify a user that an approval request they made has been resolved. Bit9 provides two ways to do this via email:

- **Manual** – You can click on the Response E-mail field on the Approval Request Details page to open a pre-configured email form in your default mailer.
- **Automatic** – You can add automatic notification to your request workflow. Automatic email notification is activated on the Mail tab of the System Configuration page. This is disabled by default.

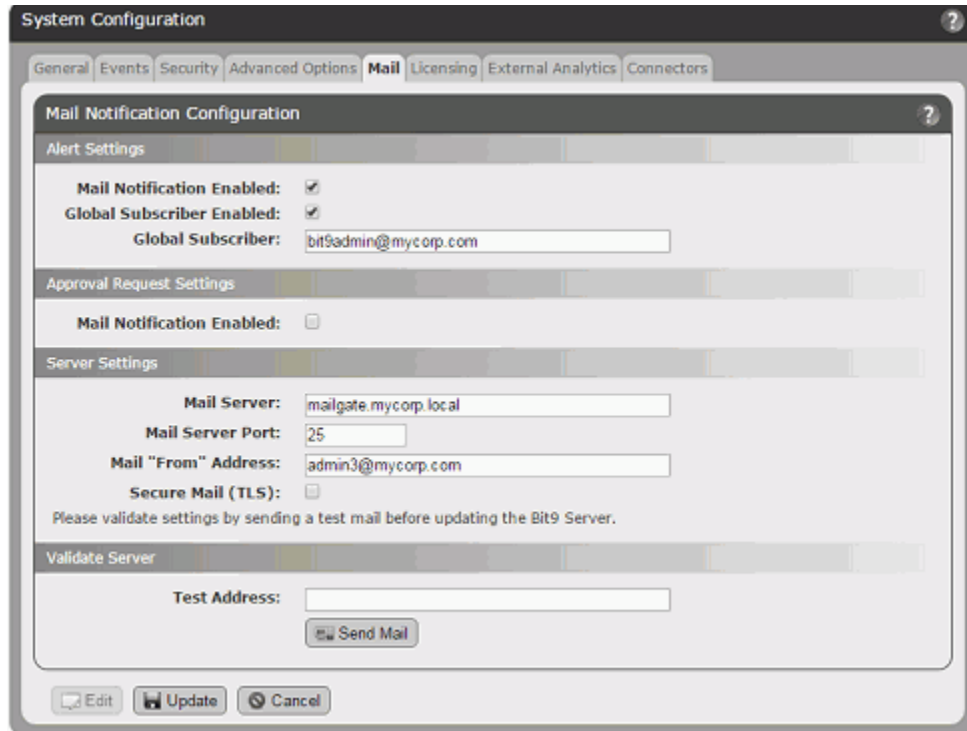
For either method, the response mail will go to the email address (if any) that the requestor provided with their request.

### Note

The automatic response features applies to Approval Requests only. No mail is sent automatically for Justifications.

### To enable automatic approval request email responses:

1. On the console menu, choose **Administration > System Configuration**, and on the System Configuration page, click the **Mail** tab.
2. In the Approval Request Settings panel, check the **Mail Notification Enabled** box.



3. If you have not already configured a mail server for the Bit9 Security Platform, provide the necessary information in the Server Settings panel and validate the server by sending a message to a test address. See [“Configuring Alert and Approval Request Mail”](#) on page 635 for more details about mail server configuration.
4. Click the **Update** button at the bottom of the page to save your settings.

### When Notifications are Sent

After the server mail configuration is correctly configured and approval request notification mail is enabled, *closing* an Approval Request causes a mail notification to be sent in the following cases:

- The Resolution field is *changed to any Resolved option* from Not Resolved or Rejected.
- The Resolution field is *changed to Rejected* from any other option.
- The Resolution field is *Not Resolved* when an open request is closed.

Notification mail is *not* sent if the Resolution field is changed from one Resolved option to another (for example, from *Resolved - Approved* to *Resolved - Updater*).

Also, notification mail is not sent unless the Status is changed to *Closed*.

When approval request notification is enabled, notifications are not sent for requests that have already been closed. However, if a request is opened for the first time (or re-opened) after notification is enabled, the requestor will be notified if the Status and Resolution fields meet the criteria above.

The Bit9 Server keeps a record of request resolution mail, including a timestamp of when it was sent from the server. This is a record of mail being sent, not received. If the email address for the recipient is incorrect, the server will still record that the message was sent.

If there is no email address for the requestor, the server *does not* indicate that mail was sent.

The record of when a request response was sent appears in the Mail Sent field. In the Approval Requests table, this is an optional column that you can add using the Show/Hide Columns feature. On the Approval Request Details page, it always appears if a message was sent.

Action	Date Requested	Requestor	Reason	Mail Sent
<input type="checkbox"/>	Oct 18 2012 01:55:23PM	MYCORP\jsmith	I use this file for testing purposes.	
<input type="checkbox"/>	Oct 17 2012 04:51:30PM	MYCORP\tjgomez	This is a new application for sales.	Oct 17 2012 04:58:48PM
<input type="checkbox"/>	Oct 17 2012 02:41:29PM	MYCORP\vjones	Driver for a new printer I bought.	Oct 17 2012 04:01:23PM
<input type="checkbox"/>	Oct 17 2012 02:38:40PM	MYCORP\srossi	Can I run this photo-management s/w?	

### Notification Mail Content

When approval request resolution mail is sent, it contains the following information:

- The filename for which the approval was requested
- The Resolution (i.e., the choice made on the Resolution menu)
- Any comments added by the Bit9 Platform administrator in the Approval Request Details.
- The reason for the request (if provided by the requestor).
- The requestor's email address
- The date of the request
- The hostname of the Bit9 Server

<b>From:</b> <a href="mailto:admin3@mycorp.com">admin3@mycorp.com</a>	
<b>Sent:</b> Wednesday, October 17, 2014 4:58 PM	
<b>To:</b> Tom Gomez	
<b>Subject:</b> Bit9 Request Approval Response on b9srv.mycorp.local: trackleads.exe is Resolved - Approved	
<b>Request Approval Response</b>	
<b>Request for "trackleads.exe" is Resolved - Approved</b>	
Approval Response:	We determined that this app is legitimate and safe.
Request Reason:	Our department will be using this new application on a daily basis.
Requested By:	<a href="mailto:tjgomez@mycorp.com">tjgomez@mycorp.com</a>
Requested On:	Oct 9 2015 12:14PM
Bit9 Platform Server:	b9srv.mycorp.local



## Approval Request and Justification Details

The following tables describe the fields on the Approval Request Details page. Note that other fields may be available as options in the Approval Request table.

**Table 66:** Request/Justification Information

Field	Description
Computer	The name of the computer on which the block occurred.
Policy	The Policy in effect for the agent computer at the time of the block.
Platform	The platform of the computer on which the block occurred.
Enforcement Level	The Enforcement Level of the Policy in effect for the agent computer at the time of the block.
Request Type	Either "Approval" or "Justification".
Requestor	The user that made the request.
Response E-Mail	The email address (if any) provided by the blocked user.
Priority	The priority of the request (as set by the user). The options are High, Medium (the default), and Low.
Rule Type	The type of rule that blocked the action. For example, "Unapproved executable" indicates that execution of an unapproved file was blocked on a computer whose policy blocks such executions.
Reason	Approval request or justification text entered in the notifier.
Comments	Comments by an administrator reviewing the request. Can be modified and updated at any point.
Resolution	How the request was resolved. The menu choices are: <ul style="list-style-type: none"> <li>• Not Resolved</li> <li>• Rejected</li> <li>• Resolved-Approved</li> <li>• Resolved-Rule Change</li> <li>• Resolved-Installer</li> <li>• Resolved-Updater</li> <li>• Resolved-Publisher</li> <li>• Resolved-Other</li> </ul> <p>The choice for this field is informational only and does not change any rules or files states. It can be changed only when the request or justification is open.</p>
Status	The status of the request. The values are: <ul style="list-style-type: none"> <li>• Submitted – A user has sent the request.</li> <li>• Open – The request has been opened by an administrator. Both Submitted and Closed requests can be opened. A request must be open for the Resolution field to be changed.</li> <li>• Closed – The request has been closed, presumably because it has been in resolved in some way. Requests can be closed even if no action has been taken to respond to them.</li> </ul>
Mail Sent	If automatic request responses are enabled and one was sent for this request, this field shows the timestamp for that mail.



The Bit9 Analysis panel shows information resulting from clicking the **Run Analysis** button. This panel provides statistics about the blocked file and the user requesting access.

**Table 67:** Bit9 Analysis of Requests and Justifications

Link/Button	Comments
<number >blocks seen by this computer within 1 hour(s).	Number of blocks on this computer in one hour time period ending at the time analysis was run. Clicking this link displays Events page filtered to show all types of block events associated with this computer
<number> blocks from this process on this computer. within 1 hour(s).	Number of blocks by the given process on this computer in one hour time period ending at the time analysis was run. Clicking link displays Events page filtered to show block events associated with the process that attempted to perform the blocked action on this computer.
<number> files written by <the process that tried to execute this file> on this machine.	Clicking link displays Find Files page filtered to show the files written by this process on this machine. <b>Platform Note:</b> This field appears only for files on Windows computers.
<number> files written by <the process that tried to execute this file> on the network.	Clicking link displays Find Files page filtered to show all instances of files written by this process on any computer. <b>Platform Note:</b> This field appears only for files on Windows computers.
File appears on <number> computers with <number> different hashes.	Search results for the name and path in the request, across all computers managed by your Bit9 Server. Clicking the link displays the Find Files page filtered to show all instances matching the file name and path.
<number> approval requests for this file.	The number of requests for this file, identified by <i>hash</i> . Clicking link displays the Approval Requests table filtered to show all requests for this file hash.
<number> total approval requests by this user.	Clicking link displays the Approval Requests table filtered to show all approval requests from this user.
<number> open requests by this user.	Clicking link displays the Approval Requests table filtered to show all <i>open</i> approval requests from this user.
Last Analysis Completed On <datetime> (Read Only)	Reports when the last analysis was run for this request, or if it has not yet been run.
Run/Rerun Analysis (button)	Runs an analysis that provides the information in this panel. If the analysis has already been run, reruns it to update any of the changed information, such as the number of requests from the user or the number of files written by the process that tried to write the blocked file.

**Table 68:** File Information in Approval Request/Justification Details

Field	Description
File Name	Clicking on link displays the File Instance Details page for the blocked file.
SHA-256	Clicking on link displays the File Instance Details page for the blocked file.
File State	The global state of this file in the Bit9 File Catalog.
Local State	The local state of the blocked file instance on this computer.
Publisher	The publisher name and publisher approval state. Clicking on the publisher name opens the Publisher Details page for the blocked file's publisher.
File Prevalence	The number of computers on which the blocked file appears.
Trust Rating	Trust rating (if known) from Bit9 SRS for the blocked file. Ranges from 0 (untrusted) to 10 (highly trusted).
Threat Level	Threat level (if known) from Bit9 SRS for the blocked file. Values are 0 (Clean), 1 (Potential Risk) and 2 (Malicious).

The Process tab and the Installer tab provide the same information for their subjects.

**Table 69:** Process and Installer Information in Request/Justification Details

Field	Description
Process	Full path to process that attempted to write or execute the blocked file.
Installer	Full path to the installer for the blocked file.
SHA-256	SHA-256 hash of the process or installer.
Trust Rating	Trust rating (if known) from Bit9 SRS for the process attempting to run the blocked file or the installer that installed the file. Ranges from 0 (untrusted) to 10 (highly trusted).
Threat Level	Threat level (if known) from Bit9 SRS for the process attempting to run the blocked file or the installer that installed it. Values are 0 (Clean), 1 (Potential Risk) and 2 (Malicious).

See [“Customizing the Request/Justification Interface in Notifiers”](#) for details about other modifications you can make.

## Customizing the Request/Justification Interface in Notifiers

You can change the text for the headings, links, and instructional text in the Approval Request panel. One reason to do this is so that different labeling appears for Approval Requests and Justifications on notifiers modified in previous releases.

### Notes

- If you add any customization tags for Approval Requests and/or Justifications, you *must* enable the feature(s) using the Approval Request menu on the Edit Notifier page.
- **Platform Note:** The Approval Request/Justification interface on the Bit9 Notifier History window can be customized only for Windows computers.

Table 70, “Approval Request and Justification Customization tags,” shows the tags that can be used to modify approval requests in notifiers. The example below, which is the Notifier Text for Block unapproved executables in the Template Policy, shows where you would put tags to have different labeling for each of them.

```
<BlockText:Bit9 blocked an attempt by <ProcessName> to run
<TargetName> because the file is not approved.  If you
require access to this file, please contact your system
administrator.><AskText:Bit9 identified and paused an
attempt by <ProcessName> to run <TargetName> because the
file is not approved.  Choose Allow to let this file run, or
choose Block to stop it from running at this
time.<NotifierRequestLink:Submit
Justification><NotifierRequestText:Enter your reason for
access.><NotifierRequestHeading:Justification><NotifierReque
stProcessed:Justification has been submitted.>  Scroll down
for diagnostic data.
```

**Table 70:** Approval Request and Justification Customization tags

Tag	Description
<NotifierRequestLink: <i>text</i> >	This text appears on the link that opens and closes the Approval Request panel in the notifier.
<NotifierRequestHeading: <i>text</i> >	This text appears above the text box into which the user types the request.
<NotifierRequestText: <i>text</i> >	This text appears inside the text box into which the user types the request. It disappears when the user begins entering the actual request.
<NotifierRequestProcessed: <i>text</i> >	After a user submits a request, this text appears inside the text box, indicating that the request was processed.
<NotifierRequireSubmitOnAllow>	If present, the Allow or Approve button in a notifier is disabled until the user submits a justification.
<NotifierRequireSubmitOnBlock>	If present, the Block button in a prompt notifier is disabled until the user submits a justification.
<NotifierRequestMinLength: <i>n</i> >	If present, the Submit button in an approval request or justification is disabled until the user enters at least <i>n</i> characters into the request/justification text box.

## Chapter 18

# Events, Alerts and Meters

This chapter explains how to use Bit9 event reports and alerts to monitor file activity and other key Bit9 operations on your network. It also describes tools for detecting propagation of files on your network and for keeping track of the number of times a specified file executes.

There are many uses for these features, individually and in combination. For example, when you are allowing computers on your network to execute unapproved files, you can track the executions by file, computer, and computer user. If you are operating entirely at High Enforcement Level, you can use Bit9 monitoring features to be sure that files are being blocked or allowed as you want. And you can connect other monitoring features to *alerts* that will automatically tell you when certain actions occur or thresholds are passed.

See also [Chapter 19, “Monitoring Change: Baseline Drift Reports,”](#) for details on Bit9’s ability to track changes in the overall inventory of files on your systems.

For information about analyzing Bit9 events and file information with your own tools, see [Appendix A, “Live Inventory SDK: Database Views,”](#) and the separate *Bit9 Events Integration Guide* document available through Bit9 Technical Support. Also see [Appendix F, “Exporting Bit9 Data for External Analysis,”](#) for information about exporting Bit9 events to external data analytics tools.

### Sections

Topic	Page
<a href="#">Monitoring Prerequisites</a>	482
<a href="#">Event Reports</a>	482
<a href="#">Viewing Reports on the Events Page</a>	484
<a href="#">Taking Action on Files in Event Reports</a>	488
<a href="#">Customizing Event Reports</a>	488
<a href="#">Using Bit9 Alerts</a>	494
<a href="#">Creating Alerts</a>	498
<a href="#">Alerts for File Prevalence</a>	514
<a href="#">Monitoring Specific File Executions</a>	516

## Monitoring Prerequisites

Accurate Bit9 event monitoring require that client computers (laptops, desktops, and servers) are online and actively monitored by Bit9 Agents. This chapter assumes the following:

- Bit9 policies have been created and configured.
- The Bit9 Agent is installed on the computers you want to monitor, and the computers have completed their initialization.
- All Bit9 Agents are at version 7.0.0 or greater.

For more information about these tasks, refer to [Chapter 5, “Creating and Configuring Policies,”](#) and [Chapter 4, “Managing Computers.”](#)

Although not a prerequisite for monitoring, if you intend to use an external event logging server, install the SQL Server on that system and configure Bit9 Server to connect to the external server (see [“Setting up External Event Logging”](#) on page 619) so that you begin capturing events on the external server as soon as possible.

## Event Reports

The Bit9 Events page provides access to all recorded events related to Bit9 activities, including files blocked, unapproved files executed, system management processes and actions by console users. The Bit9 Server updates event data in near-real-time for connected computers, with minor variations due to event volume.

There are predefined Bit9 reports, available on the Saved Views menu, and you also can create and save your own Saved Views using existing views as templates or starting with the full events table. For any event report, you can change the window of time for which you want results without having to create a new Saved View.

The Events page displays up to 200 events per page for the time period you specify. You can adjust the number of events displayed in a table by changing **rows per page** parameter in the bottom right of the page.

### Notes

You can optionally choose to direct the Bit9 Syslog event output for postprocessing on another system. If you do so, event output also remains displayed in the Bit9 Console event log. For more information, please refer to [Event Management Options](#) in the Bit9 Configuration chapter.

You also can export Bit9 events to a folder for use by external data analytics products. See [Appendix F, “Exporting Bit9 Data for External Analysis,”](#) for details.

See *Bit9 Events Integration Guide*, a separate document available from Bit9, for a complete list of events and mapping instructions for output to supported Syslog formats.

## Using the Home Page Event Reports Portlet

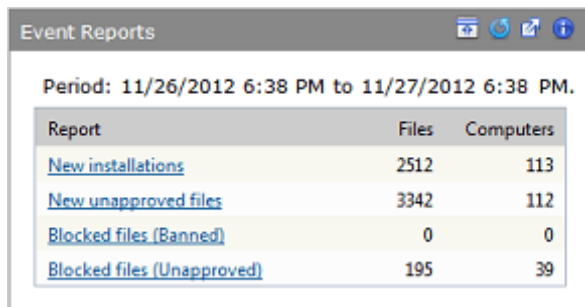
One way to monitor events is to use the Event Reports portlet on the Bit9 Console Home Page. The summary provides basic data from and links to the following four predefined Saved Views on the Events page – the views are described in more detail in [“Viewing Reports on the Events Page”](#) on page 484:

- New installations (*Windows only*)
- New unapproved files
- Blocked files (Banned)
- Blocked files (Unapproved)

The portlet shows the number of files and/or computers involved in events of each type over the previous 24 hours. This data is updated when you display or refresh the page, and you can get the full report by clicking on the report name.

### To display the Home page daily event summary:

1. On the console menu, click **Home Page**. By default, the Event Reports portlet appears in the lower left of the page.



Report	Files	Computers
<a href="#">New installations</a>	2512	113
<a href="#">New unapproved files</a>	3342	112
<a href="#">Blocked files (Banned)</a>	0	0
<a href="#">Blocked files (Unapproved)</a>	195	39

2. From the Event Reports portlet, click a report name to go to the Saved View on the Events page with the full report. See [“Viewing Reports on the Events Page”](#) for more information.

### Note

You can create custom event portlets for display on the Home Page or another dashboard. See [“Using and Customizing Dashboards”](#) on page 567 for more details.

## Viewing Reports on the Events Page

All event reports available on your Bit9 Server, whether provided by Bit9 or created at your site, appear as *Saved Views* on the Events page. [Table 71](#) lists the predefined Saved Views and the events they include.

**Table 71:** Saved Views on the Events Page

Menu Choice	Description
<b>(none)</b>	Displays a report showing an unfiltered view of all Bit9 events during the selected time period, with default columns.
<b>Alerts and Meters</b>	Displays a report that includes all creation, modification, or deletion of alerts or meters, plus all activity that triggers an alert or increments a meter (during the selected time period).
<b>Approval Requests</b>	Displays a report that includes each time an approval request for a blocked file is created (on an agent computer) and opened or closed (in the Bit9 Console).
<b>Blocked Files (All)</b>	Displays a report that includes all files blocked for any reason (or that would have been blocked but are in Report Only state) during the selected time period. This includes files that are explicitly banned, files in an unapproved state that were blocked because of a particular computer's Enforcement Level or policy, files that have not been analyzed yet, files on blocked devices, and files blocked because of custom rules.  Actions blocked by registry or memory rules and certain built-in internal Bit9 protection do not appear on this list.
<b>Blocked Files (Banned)</b>	Displays a report that includes all files that have been blocked on computers running the Bit9 Agent during the selected time period due to an explicit ban on the file.
<b>Blocked Files (Report Only)</b>	Displays a report that includes all files that would have been blocked during the selected time period but are in Report Only state due to the combination of policy settings and Enforcement Level for the computer executing them.
<b>Blocked Files (Unapproved)</b>	Displays a report that includes all Unapproved files that have been blocked during the selected time period as a result of a policy's Unapproved Executables or Unapproved Scripts setting and its applied Enforcement Level.
<b>Carbon Black</b>	When a Carbon Black server is integrated with a Bit9 Server, displays a report that includes all watchlist events from the Carbon Black server and status events from Carbon Black sensors.
<b>Computer Management</b>	Displays a report that includes the events for the selected time period related to computers running the Bit9 Agent, including new and deleted computers; agent startup and shutdown; computers moved to a different policy; changes in policy's settings or Enforcement Level; and changes in the AD policy mapping rules (including their order).



Menu Choice	Description
<b>Connectors</b>	Displays a report that shows network security connector-related events, such as external notifications, malicious file detections, file analysis activity, and the addition, configuration, and removal of connector integrations.
<b>Console Access</b>	Displays a report that includes user logins and logouts, and creation, editing, and deletion of console login accounts during the selected time period.
<b>Device Control</b>	Displays a report that includes device-related events during the selected time period. These events include approving, banning or removing approvals or bans on devices, detection of a new device on the network, detection of attachment or detachment of a device on the network, and any device access covered by device-related policy settings. <b>Platform Note:</b> Device control is effective for Windows computers only.
<b>Duplicate Computer Registrations</b>	Displays a report that includes all events involving attempts to register more than one computer under the same agent id.
<b>File Analysis</b>	Displays a report that includes all events related to file analysis by external tools. This includes external notifications, file upload events, and reports of malicious or potential risk files from Bit9 SRS or third-party tools.
<b>Memory</b>	Displays a report that includes all events related to memory (process protection) rules. <b>Platform Note:</b> Memory rules affect Windows systems only.
<b>New Files (All)</b>	Displays a report that includes all new files (i.e., not previously in the File Catalog) that have appeared on computers at your site during the selected time period.
<b>New Files (Approved)</b>	Displays a report of all files approved because of various reasons during the selected period. Does not include files approved because of initialization.
<b>New Files (Banned)</b>	Displays a list of all new banned files seen on the network.
<b>New Files (Unapproved)</b>	Displays a report that includes all new files that have appeared on the server during the selected time period and have not been approved or banned.
<b>New Installations</b>	Displays a report that includes each instance in which a file writes one or more files (creating a new file group) during the selected time period. <b>Platform Note:</b> Includes Windows installations only.
<b>Registry</b>	Displays a report that includes all events related to Windows Registry rules. <b>Platform Note:</b> Registry rules are applicable to Windows computers only.
<b>Reputation</b>	Displays a report that includes all reputation-related events, including adding or deleting a file or publisher approval based on reputation, or changes to file or publisher reputation properties.

Menu Choice	Description
<b>Security Alert Events</b>	Displays a report of security-alert-related events. Events include agent computers unprotected by Bit9 because of upgrade failures, detection or prevention of agent tampering, and a computer clock out of sync (potentially set back to attempt to defeat security measures.).
<b>Server Management</b>	Displays a report that includes any modifications to data on the System Configuration pages, data related to Bit9 database backup (success, failure, changes), server errors, Bit9 SRS errors, database errors, and startup or shutdown of the Bit9 Server (during the selected time period).
<b>System Health History</b>	Displays a report that includes any changes in the severity of a health indicator as well as any creation, modification or deletion of health indicators.
<b>Temporary Policy Overrides</b>	Displays a report that includes each time a temporary policy override code is generated for an agent.
<b>Threat Indicators</b>	Displays threats detected by the ATIs in the Indicator Sets on Bit9-managed computers. If no Indicator Sets have been activated, this view will be empty. See <a href="#">Chapter 20, "Advanced Threat Detection,"</a> for more information about this and other threat-related event views.
<b>Threat Indicators - Legacy</b>	Displays threats detected by the ATIs that were installed in releases prior to v7.2.0. If you did not install the Detection Enhancement in a prior release, this view will be empty.
<b>Threat Report - Suspicious Executable Created by Shell</b>	Displays events in which certain executable files are created by cmd.exe or powershell.exe in locations such as the system directory, RecycleBin, or AppData.
<b>Threat Report - Suspicious Files by Location</b>	Displays events in which a file is first seen or executed on any computer, or first appears (unapproved) on at least one computer, in an unusual, suspicious location. An example would be unexpected file activity in the Recycle Bin.
<b>Threat Report - Suspicious Files by Name</b>	Displays events in which a file is first seen or executed on any computer, or first appears (unapproved) on at least one computer, with a suspicious name, often a name that appears similar to the name of a legitimate Windows file. For example, discovery of a file named svch0st.exe (using a zero in place of the lowercase 'o' in svchost.exe) would appear in this event view.
<b>Threat Report - Suspicious Files by Parent</b>	Displays events in which an unknown, or low prevalence, executable file is written by a program that should not normally be creating such files. An example of this would be an executable file created by Adobe Reader; this is often indicative of a malformed- or malicious-PDF-style attack.

**To view an existing Bit9 Event report:**

1. On the console menu, choose **Reports > Events**. The Events page appears with the default view showing all events in the past hour:

The screenshot shows the Bit9 Events page. At the top, there are controls for 'Saved Views' (set to '(none)'), 'Group By' (set to '(none)' and 'Ascending'), and 'Max Age' (set to '1 day'). Below these are links for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', 'Access Event Archives', and 'Refresh Page'. A search bar is present with a search icon and a search button. The main area is a table of events with the following columns: Timestamp, Severity, Type, Subtype, and Description. The table contains 13 rows of event data.

Timestamp	Severity	Type	Subtype	Description
Mar 13 2015 05:20:04PM	Notice	Discovery	New publisher found	New publisher found: 'Tech Corporation'.
Mar 13 2015 05:17:39PM	Notice	Computer Management	Agent Enforcement Level changed	Computer 'MYCORP\DESKTOP-37' change
Mar 13 2015 05:17:21PM	Notice	Computer Management	Agent policy changed	Computer 'MYCORP\DESKTOP-37' change
Mar 13 2015 05:17:21PM	Info	Computer Management	Computer modified	Computer 'MYCORP\DESKTOP-37' was m
Mar 13 2015 05:17:07PM	Info	Policy Management	Policy created	Policy 'Monitor' was created by 'admin'.
Mar 13 2015 05:17:07PM	Notice	Policy Management	Install package created	An install package Monitor.msi was create
Mar 13 2015 05:16:13PM	Notice	Policy Enforcement	Execution block (unapproved file)	File 'd:\setup.exe' [6270B...81F30] was blc
Mar 13 2015 05:16:13PM	Notice	Discovery	New unapproved file to computer	Computer MYCORP\LAPTOP-115 discover
Mar 13 2015 05:12:51PM	Notice	Discovery	New publisher found	New publisher found: 'Sun Microsystems, I
Mar 13 2015 05:12:19PM	Info	Session Management	Console user login	User 'admin' logged in from ff11:c1:234:3
Mar 13 2015 05:09:28PM	Info	Discovery	Device attached	Device 'VMWARE_ VMWARE_VIRTUAL_S (S/
Mar 13 2015 05:08:57PM	Notice	Discovery	New device found	A new device 'MAGICISO VIRTUAL_DVD-RO
Mar 13 2015 05:08:56PM	Info	Computer Management	Agent restart	Bit9 Agent has started, version 7.2.0.547

2. Select a view from the Saved Views menu. The view appears. For views with many, and in some cases, wide columns, you might need to scroll left and right to see all the data for an event.

See [“Customizing Event Reports”](#) on page 488 for details about changing and saving reports.

**Notes**

- You can download event tables in CSV format.
- If an IP address is listed in an event table or description, it is the IP address of the agent computer at the time the event was reported, which is not necessarily the current IP address.

**Object Previews in Events Tables**

As in other tables, if an item in the Events table is highlighted, you can click on it for more details. You also can hover the cursor over many highlighted items to see an Object Preview, which provides summary information without navigating away from the page.

The screenshot shows an Object Preview for a File Instance. The preview is a white box with a blue title 'File Instance' and contains the following information:

- File Name:** reader10manifest.msi
- File Path:** c:\programdata\adobe\arm\reader\_10.1.9\reader\_10.1.9
- Computer:** MYCORP\Laptop-3
- Global State:** Approved
- Local State:** Approved

Below the preview, a table shows the event details:

Type	Subtype	Description
Policy Enforcement	File approved (custom rule)	File 'c:\programdata\adobe\arm\reader_10.1.9\reader10manifest.msi' [EF4FF...5DD70] was approved due to custom rule.
Policy Enforcement	File approved (custom rule)	File 'c:\programdata\adobe\arm\reader_11.0.10\reader11manifest.msi' [18E93...24479] was approved due to custom rule.

## Taking Action on Files in Event Reports

Whenever the details of an event identify a file, you can take action on that file directly from the Events page. To do this, you check the checkbox to the left of the event in the table and then choose an action from the Action menu. Only events containing file information can be checked.

The actions you can take on a file on the Events page are the same as those you can take on the Files page, including:

- Locally approve a file instance or remove local approval
- Globally approve or ban a file for all computers
- Create a custom approval or ban that applies to computers in specific policies
- Create a report-only ban that only reports that it *would have blocked* the file if fully enabled
- Remove an approval or ban
- Analyze the file by getting Bit9 Software Reputation Service (SRS) information

See [Chapter 8, “Approving and Banning Software”](#) for details on these file actions.

If the Bit9 Connector option is installed and licensed, you also can upload files or analyze them with a third-party network security appliance. See [Appendix C, “Bit9 Connector for Network Security Devices”](#) and [Appendix E, “Uploading Files from Agents”](#) for details.

## Customizing Event Reports

Several Saved Views are available on the Events page. In any view, you can use the Show/Hide Filter and Show/Hide Columns buttons to customize what you see, for instance, choosing to show events for a particular platform. You can also use the Show/Hide buttons to determine whether a table you are viewing has already been modified.

If you want a special report for one time use, you can simply make the customizations, view the results, and *not* save the changes. If you have made unsaved changes, a message next to the Saved Views menu reports that and offers you the option of discarding the changes. Depending upon the setting for Remember Page Settings on the Bit9 Console Preferences page, when you leave and return to the Events page, your view may be filtered to show these customizations even when not saved.

To save a custom report, use the Saved View panel and either save it under the an existing Saved View name (if it is not a built in Bit9 report) or under a new name.

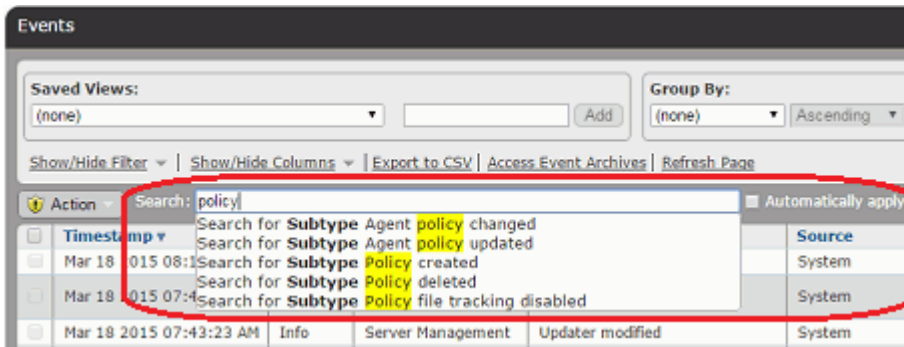
For more information on console table features, see [Bit9 Console Tables in Chapter 2, “Using the Bit9 Console.”](#)

## Using the Event Search Box

The Events page includes a Search box that helps you quickly locate events matching strings you enter. Search strings are matched against data in the following fields:

- File Hash
- Source
- Subtype
- Platform
- IP Address

If any data in these fields in the Events database matches the string, an auto-completion menu provides a list from which you can select the item you wanted to see.



When you choose an item from the list, the table is filtered in one of two ways:

- If you checked *Automatically apply* before entering the search screen, clicking on an option in the menu immediately filters the table to show only events matching that string in the appropriate field.
- If you did not check *Automatically apply*, clicking on an option in the menu opens the Show/Hide Filters panel with a filter configured to show only events matching that string in the appropriate field. You can add other filters if you choose before applying the changes to the table view.

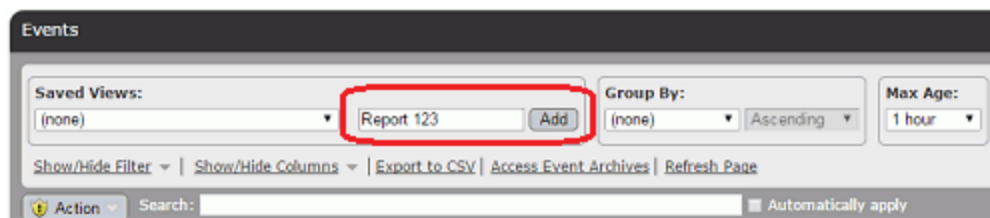
**Table 72:** Event Report Parameters

Field	Description
<b>Saved View</b>	Name for this report. If you are creating a new report, enter any text that indicates the purpose of the report in the <i>right</i> text box of Saved Views and then click <b>Add</b> . The report is saved and listed by its new name in the Saved Views menu with the other reports.
<b>Maximum age</b>	Time period of interest. You see events in the report between the time the report is run and a specified period in the past (hours, days, weeks, or months). Your choice takes effect immediately. Note that the Filters panel allows you more options for setting a time window, including <b>Timestamp</b> , for which the start and/or end date does not have to be the current date and time.
<b>Rows per page</b>	Maximum number of events displayed on a single page in the Events table. This is controlled on a per-user basis by the <i>rows per page</i> menu in the bottom right below the table. Default value is 25. If your report includes more items than the <i>rows per page</i> setting, The console creates more pages and a page number panel for navigation.
<b>Group by</b>	Column by which you want to group like results for default display and the sort order (ascending or descending). <i>Group by</i> creates expandable lists that initially only show the group name (for example, security policies) and number of items per group, but can be clicked to show the members of the group (for example, computers). Not all column names are available for grouping.

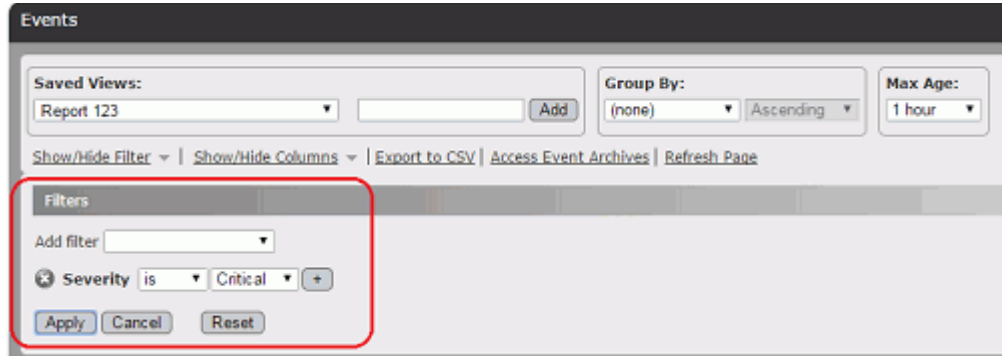
Field	Description
<b>Filters</b>	<p>Event parameters you want to apply to the report. You can specify any combination of filters to determine which events are included in a report.</p> <p>Although most of the filters are for data clearly associated with the file or computer in the event, the following are special cases:</p> <p><b>Subtype</b> – Subcategories of events for all Bit9 event types. You can specify one or more event subtypes for display. If you select no subtype, the console searches for all.</p> <p><b>Severity</b> – filter enables you to show or hide events based on standard Syslog message severity guidelines, categorized as follows:</p> <ul style="list-style-type: none"> <li><b>Critical</b> – critical conditions</li> <li><b>Debug</b> – debug-level messages</li> <li><b>Error</b> – error conditions</li> <li><b>Info</b> – informational messages</li> <li><b>Notice</b> – normal but significant condition</li> <li><b>Warning</b> – warning conditions</li> </ul> <p>Severity status for each log message is shown in the Severity column.</p> <p><b>Note:</b> In previous releases, the column and filter now labeled Severity was called “Priority”.</p>
<b>Columns</b> (Show/Hide)	<p>Information to be included as columns in the Events table. Use arrows to specify which columns are displayed and in what order: Items in the <i>Selected</i> list are displayed in the table. Items in the <i>Available</i> list are not displayed in the table.</p>

### To customize and save an event report as a Saved View:

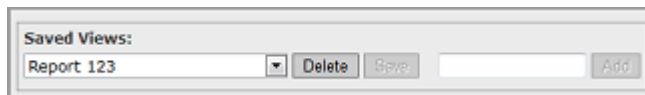
1. In the console menu, choose **Reports > Events**. The Events page appears.
2. If one of the existing reports in Saved Views is similar to the report you want, choose it from the Saved Views menu. Otherwise, choose **(none)**.
3. Click in the right box of the Saved Views panel, type in a report name, and click **Add**. The new report now appears as the current Saved View and is added to the menu. Note that you also can wait until you have made all of your changes to create the new view.



4. Click the **Show/Hide Filters** link and choose one or more filters to specify the parameters for your report. You can add as many filters as you need. Click **Apply** when you are finished configuring filters.



5. Click the **Show/Hide Columns** link and use the arrow buttons to choose which types of data you want to display in your report, and the order in which you want them to appear. Click **Apply** when you are finished adding and removing columns.
6. If you did not choose the time range for your report during filter configuration, choose time span from the *Maximum Age* menu.
7. If you would like a different number of rows per page than currently shown, use the *rows per page* dropdown menu in the bottom right of the page.
8. If you would like the data in your report collapsed into expandable group, choose a group and sort direction (ascending or descending) in the *Group by* menus. For example, if you Group by Policy, the Events page initially shows Policy names, and you click on the Policy name to show the events for computers in that policy.
9. When the report is formatted as you want it, make sure the name you want to use for it is showing in the Saved Views menu and click the **Save** button in the Saved Views panel. Your report is saved with the changes you specified.



## Editing Event Reports

Editing a report is similar to creating one, except that you keep the same report name.

### Note

The pre-defined Saved Views provided with the Bit9 Server are Read Only. You cannot modify them and save them under the same name; you can modify them and save them under a different name.

### To edit an existing event report:

1. In the console menu, choose **Reports > Events**. The Events page appears.
2. From the Saved Views menu, select the report you want to edit. The report appears.
3. Make all of the changes you want in the report (see [Table 72, “Event Report Parameters”](#) on page 489) and then click the **Save** button.



## Adding Command Line Information to Event Reports

You may be interested in the command lines for processes referenced in events generated by Bit9 agents. Although it is not part of the default Event Page views, a Command Line column can be added to the Events page using the Show/Hide Columns panel. In addition, command line data is accessible through the Bit9 Live Inventory SDK. It is *not* currently included in Syslog output from the Bit9 Server.

When there is a process associated with an 7.2-agent-generated event, the Command Line field will show the first 512 characters of a process command line. Pre-7.2.0 agents will not provide this information.

Subtype	Command Line
Execution block (unapproved file)	"C:\Windows\system32\cmd.exe"
Execution block (unapproved file)	C:\Windows\Explorer.EXE
Execution block (unapproved file)	C:\Windows\SysWOW64\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v2.0"
File approved (publisher)	"C:\Program Files (x86)\Bit9\Parity Console\php\php-cgi.exe"

The command line shows the process that attempted the action, not the file that was acted upon. In the example above, the first two lines show that execution of a script was blocked. In the first case, a user attempted to run the script from a command prompt. In the second, the user double-clicked on the script.

To capture command line data for actions that do not normally produce events, you can add a Custom Rule to report for those actions. On the Add Custom Rule page, you choose **Advanced** as the Rule Type, **Execute** (or Execute and Write) as the Operation, and **Report Process Create** as Execute Action. Then enter the Process and Path or File information for the process that may be created by the initiating process. Actions matching the rule will report events (including command line information) upon process creation.

### Important

- Command line data may include sensitive information such as passwords. While the Command Line column heading will appear to all users if added to a view, only users with specific permission will see any data in the column or in any data exported to a CSV file. This permission, which is called *View process command lines*, is not enabled by default for any of the console login account groups, and should be enabled only for users that need it. See [“Account Group and Access Privileges”](#) on page 76 for details about changing the permissions for a user account.
- This permission has no effect on events in Syslog or Live Inventory SDK output, which always include command line data if available.
- The potential for revealing password data in this field should be kept in mind when using the Bit9 agent management commands. If you configured a password for these commands (as described in [“Configuring Agent Management Privileges”](#) on page 615), putting the command and password on one line means that the password will be included in command line field for an event. Bit9 recommends that you enter the agent management command alone, and then provide the password at the prompt that follows.



## Viewing Install Event Details

If an event subtype is highlighted, the event has other events associated with it. Clicking on a highlighted event subtype brings you to an Install Event Details report, which shows all of the sub-events associated with the event you clicked (per computer). The Details report is useful primarily to show the *connections* between a root event and the events it generates.

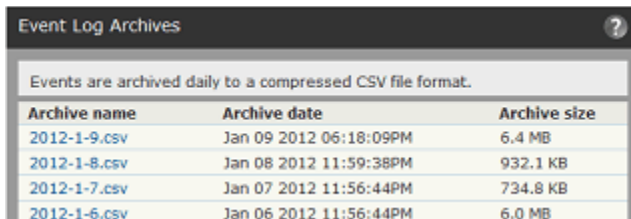
### Note

It is *events* generated by the root installation *event* that are reported here, not *files installed* by an *installer*. Whether installation of a file generates an event depends on the approval status of the installer, and may also depend upon the security policy on the computer where the files are being installed and other rule and configuration settings that can exclude file tracking. Events include information such as process name and user running the process.

Approved installers generate locally approved files, and approved files do not generate sub-events on the Install Event Details page. *Unapproved* installers generate unapproved files (unless previously approved by some other means), and unapproved files do generate sub-events. Also, any newly installed files that are blocked generate Install Event Details.

## Viewing Event Archives

The **Access Event Archives** link on the Events page opens a table of daily archives for Bit9 events. These events are archived in CSV files.



Archive name	Archive date	Archive size
<a href="#">2012-1-9.csv</a>	Jan 09 2012 06:18:09PM	6.4 MB
<a href="#">2012-1-8.csv</a>	Jan 08 2012 11:59:38PM	932.1 KB
<a href="#">2012-1-7.csv</a>	Jan 07 2012 11:56:44PM	734.8 KB
<a href="#">2012-1-6.csv</a>	Jan 06 2012 11:56:44PM	6.0 MB

You can open or download any day's event archive by clicking on the CSV file name and making your choice of action from the dialog box. These archives are located in the "archivelogs" folder under your Bit9 Server installation directory.

To return to the Events page, choose **Reports > Events** in the console menu.

### Notes

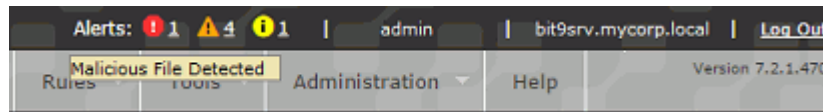
- Archiving can be enabled or disabled on the Events tab of the System Configuration page. See "[Managing the Bit9 Event Database](#)" on page 618 for more information.
- Unlike event times in the Bit9 Console, timestamps for the archived events listed in the CSV files are shown in UTC time.

## Using Bit9 Alerts

Alerts notify you of important Bit9-monitored activities, such as the appearance or spread of risky files on your computers. When conditions specified in an alert are met, notifications can be provided in the following ways:

- **Notification in Console Banner** – If any alerts are triggered, indicators appear on all console pages, in the upper right above the console menu. There are three different symbols that can appear in the banner, each representing a different alert priority, and the number of triggered alerts in each category is shown to the right of its symbol. See “[Alert Priority](#)” on page 504 for more on details on priority.

Hovering the mouse cursor over a symbol or the number to its right shows a tooltip describing either the type of alert (if there is only one in that priority) or its priority. Clicking on the symbol or number opens the Alert Instances page if one alert is triggered or the Alerts page filtered to show those alerts if more than one alert is triggered at that priority level.



- **Email Notification** – Email notification about the event(s) triggering the alert goes to a list of subscribers.
- **Alerts Page Row Highlighting** – On the Alerts page, the row for each triggered alert is highlighted, with the highlight color indicating the alert priority (red for high, orange for medium, yellow for low).
- **Home Page and other Dashboards** – All currently triggered alerts appear in the Triggered Bit9 Alerts portlet, which is part of the default Bit9 Console Home Page and can be added to other Dashboards. This portlet also uses the color and symbol coding for alert priority.

You can *reset* an alert when you no longer want to be notified about it. This removes the warning banners on the Alerts and Home pages (and any dashboard with the Triggered Alerts portlet), and if you have enabled automatic re-sends of alert email, it stops those. If the conditions that triggered the alert occur again, another alert will be triggered. If the conditions that caused the Alert cease to exist, the Alert will be auto-reset to a non-triggered state (see “[How Alerts are Triggered](#)” on page 505 for details).

An Alert History is kept for each alert, and this history is modified as alerts are triggered and reset.

### Note

Access to alert features is determined by the *View alerts* and *Manage alerts* permissions on the Login Accounts Add/Edit Group pages.

There are two top-level classes of Bit9 alerts:

- **Built-in Alerts** – [Table 73](#) shows the alerts pre-configured and listed by default in the console.
- **User-Created Alerts** – You can create and edit alerts through the Alerts page. This is described in “[Creating Alerts](#)” on page 498.

The Alerts page lists all currently available alerts, including built-in and user-created, and both enabled and disabled.

Priority	Name	Type	Enabled	Priority	Date Triggered	Date Created	Created By
<b>Priority: High</b> 5 items							
	Bit9 SRS Unavailable Alert	System Alert	No	High	Nov 04 2014 11:21:42AM	Oct 22 2014 11:29:00AM	System
	Malicious File Detected	File Security Alert	No	High	Nov 03 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	Database Limit Alert	System Alert	Yes	High	Oct 30 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	Backup Missed Alert	System Alert	Yes	High	Oct 25 2014 08:32:16PM	Oct 22 2014 11:29:00AM	System
	Database Verification Failed	System Alert	Yes	High	Oct 25 2014 08:32:16PM	Oct 22 2014 11:29:00AM	System
<b>Priority: Medium</b> 3 items							
	Console Login Alert	Event Alert	Yes	Medium	Nov 06 2014 10:08:14AM	Nov 05 2014 09:09:31PM	admin
	Computer Security Alert	Security Alert	No	Medium	Nov 03 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	File Propagation Alert	File Activity Alert	No	Medium	Oct 25 2014 08:32:16PM	Oct 22 2014 11:29:00AM	System
<b>Priority: Low</b> 6 items							
	Block Propagation Alert	File Activity Alert	No	Low	Oct 26 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	Approval Request Alert	Approval Request Alert	No	Low	Oct 26 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	Updater Modified Alert	System Alert	Yes	Low	Oct 26 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	New Certificate Alert	Certificate Alert	No	Low	Oct 26 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	Indicator Set Alert	Event Alert	No	Low	Oct 26 2014 07:32:16PM	Oct 22 2014 11:29:00AM	System
	[Sample] Windows File Properties	Event Alert	No	Low	Oct 25 2014 08:32:16PM	Oct 22 2014 11:29:00AM	System

**Table 73:** Built-in Alerts

Alert	Description
<b>Database Limit Alert</b>	Alerts subscribers when SQL Express database size reaches its specified limit (varies depending upon SQL edition). Only active if you have installed SQL Server Express edition (not a full SQL version). Always enabled (cannot be disabled).
<b>Backup Missed Alert</b>	Alerts subscribers when Database backup was scheduled but missed. Enabled by default, but can be disabled.
<b>Database Verification Failed</b>	Alerts subscribers when the Bit9 database is found to be corrupt. If triggered, contact Bit9 Support. Always enabled (cannot be disabled).
<b>Potential Risk File Detected</b>	Alerts subscribers when a file on an computer monitored by a Bit9 Agent is considered potentially malicious by Bit9 SRS or a connected security device or service. Disabled by default.
<b>Malicious File Detected</b>	Alerts subscribers when a file on a computer monitored by a Bit9 Agent is considered malicious by Bit9 SRS or a connected security device or service. Can be configured to ignore banned and/or approved files. Disabled by default.
<b>Elevated Privilege: Install Mode</b>	Alerts subscribers when any computer remains in local approval mode longer than a specified time period. The default is 1 hour, but can be modified. No computer should remain in approval mode longer than is necessary to install software.

Alert	Description
<b>Bit9 Software Reputation Service Unavailable Alert</b>	<p>Alerts subscribers when expected Bit9 SRS tasks are not performed during a period of time specified in the alert. The default period is three hours, but you can modify this. Enabled by default if Bit9 SRS is activated (and cannot be disabled). Disabled if Bit9 SRS is not activated.</p> <p>Once triggered, the alert remains in effect until all standard Bit9 SRS tasks are restored to normal operation. It can be manually reset, but will trigger again after the specified period if the conditions that caused the alert still exist.</p> <p>The conditions that trigger this alert also add a notification that Bit9 SRS is unavailable to the System Configuration/Licensing page.</p>
<b>Approval Request Alert</b>	<p>Alerts subscribers when more than the specified number of approval requests are in Submitted or Open state. Requests older than one week and Closed requests are not considered when triggering the alert. Once triggered, the alert remains in place until it is manually reset or enough requests are Closed to bring the total below the threshold. Enabled by default.</p>
<b>Justification Alert</b>	<p>Alerts subscribers when more than the specified number of justifications are created for files that endpoint users chose to allow to run. Justifications older than one week are not considered when triggering the alert. Once triggered, the alert remains in place until it is manually reset or enough justifications are Closed to bring the total below the threshold. Enabled by default.</p>
<b>Updater Modified Alert</b>	<p>Alerts subscribers when an updater is created, modified or deleted by Bit9 SRS. Always enabled (cannot be disabled).</p> <p><b>Note:</b> Automatic updater management by Bit9 SRS must be enabled on the Advanced Options tab of the System Configuration page.</p>
<b>Computer Security Alert</b>	<p>Alerts subscribers when suspicious behavior is detected on a computer. Triggering conditions include detection of a computer that is unprotected due to an upgrade failure, agent tampering detected or prevented, and a computer clock out of sync with the Bit9 Server. Always enabled (cannot be disabled).</p> <p>See <a href="#">“Detecting Agent Issues with Computer Security Alerts”</a> on page 512 for more details on these alerts and the conditions that cause them.</p>
<b>New Certificate Alert</b>	<p>Alerts subscribers when a file with a certificate for a publisher not yet listed in the Bit9 Console is discovered, or a new certificate is imported directly into the Bit9 Server. By default, this alert is triggered when a new certificate for <i>any</i> publisher is detected. However, it can be configured to trigger only for new certificates for specific publishers.</p> <p>If set to Specific Publisher, you must provide a string that matches all or part of the name of the publisher for which you want alerts. For example, if you provide “Apple” as the string, it will alert you about new certificates whose publisher is identified as “Apple”, “Apple, Inc.”, “Big Apple, Ltd.”, etc.</p> <p>You can add multiple publishers (or partial names) to the alert. Requires v7.0.1 or later agent. Disabled by default.</p>

Alert	Description
<b>Revoked Certificate Alert</b>	<p>Alerts subscribers when a certificate known to this Bit9 Server is revoked. By default, this alert is triggered when a certificate for <i>any</i> publisher is revoked. However, it can be configured to trigger only for specific publishers.</p> <p>If set to Specific Publisher, you must provide a string that matches all or part of the name of the publisher for which you want alerts. For example, if you provide "Apple" as the string, it will alert you about revoked certificates whose publisher is identified as "<i>Apple</i>", "<i>Apple, Inc.</i>", "<i>Big Apple, Ltd.</i>", etc.</p> <p>You can add multiple publishers (or partial names) to the alert.</p> <p>Requires v7.0.1 or later agent. Disabled by default.</p>
<b>Indicator Set Alert</b>	<p>Alerts subscribers when a detection indicator set is created, updated, or deleted.</p>
<b>System Health OER Alert</b>	<p>Alerts subscribers when the environment for this server is out of compliance with the Bit9 Platform <i>Operating Environment Requirements</i>, which can indicate immediate or potential performance issues.</p> <p><b>Note:</b> This alert only appears and can only be triggered if System Health Indicators are enabled on the Advanced tab of the System Configuration page and this indicator has been downloaded to the server. If present, it is always enabled.</p>
<b>System Health Infrastructure Configuration Alert</b>	<p>Alerts subscribers when the conditions in your server environment trigger a Health Indicator on the Infrastructure Configuration tab of the System Health page.</p> <p><b>Note:</b> This alert only appears and can only be triggered if System Health Indicators are enabled on the Advanced tab of the System Configuration page and this indicator has been downloaded to the server. If present, it is always enabled..</p>
<b>[Sample] Windows File Properties</b>	<p>Alerts subscribers when an the <i>Report write (custom rule)</i> occurs and triggers the Windows File Properties Indicator Set for threat detection.</p> <p>Disabled by default.</p>

## Creating Alerts

You can create and configure alerts of the following types:

**Table 74:** User-Creatable Alert Types

Alert Type	Description
<b>File Activity: Propagating File</b>	Alerts subscribers when a <i>locally unapproved</i> file appears on more than a percentage of computers for the policies and time period you specify. If you are not operating in High Enforcement, propagating files can indicate a spreading virus.
<b>File Activity: Blocked File</b>	Alerts subscribers when the same file is blocked on more than a specified percentage of computers for the policies and time period you specify.
<b>Baseline Drift Alert</b>	Alerts subscribers when baseline drift of files reaches the specified threshold.
<b>File Prevalence Alert</b>	Alerts subscribers when a <i>specified</i> file is present on more than a specified number of computers.
<b>Event Alert</b>	Alerts subscribers when specified events occur, or a specified event rule is triggered, more than a threshold number of times in the specified time period.

**To create an alert:**

1. In the console menu, choose **Tools > Alerts**. The Alerts page, which lists all currently available alerts (both enabled and disabled), appears:
2. From the Alerts page, click the **Add Alert** button. The Alert Information page appears:

3. In the Alert Information panel, enter the information requested. See [Table 75](#) below for details on the parameters you can specify.
4. When you have finished entering all the alert parameters, click either **Create**, to create the new alert and stay on this page, or **Create & Exit** to return to the table of alerts. You might use Create if you want to add subscribers to this alert.

Once created, the new alert appears on the Alerts page. If the alert is Enabled, it begins monitoring activity on your network and will trigger if it finds conditions matching the definition you set up.

**Table 75:** Alert Parameters

Section	Field	Description
<b>General</b>	<b>Alert name</b>	Name for the Alert as you would like it to appear in the Alerts table.
	<b>Message</b>	Message to be sent when alert is triggered. You can add tags to the message for an Event Alert so that it provides data specific to the alert instance. See <a href="#">“Informational Tags for Event Alert Messages”</a> on page 503
	<b>Priority</b>	Priority level assigned to this alert. The choices are: High, Medium, Low. Priority level determines the color assigned to the alert in the user interface, and allows you to group alerts by priority to highlight the most critical items.
	<b>Status</b>	Specifies whether the alert is enabled (on) or disabled (off). Note that if you disable an alert after it is triggered, this does not automatically reset the alert.
<b>Type</b>	<b>Type</b>	Type of alert you want to configure: <ul style="list-style-type: none"> <li>• File Activity: Propagating File</li> <li>• File Activity: Blocked File</li> <li>• Baseline Drift Alert</li> <li>• File Prevalance Alert</li> <li>• Event Alert</li> </ul>
	<b>Description</b>	Read-only text with more information about the specified alert Type.
	<b>Mail Template</b>	Template you want to use to determine the format and content of the email you send subscribers of this alert. The default template can be used for any alert, but the other standard templates may be more appropriate for the alert type they represent: <ul style="list-style-type: none"> <li>• Default</li> <li>• Template for File</li> <li>• Template for Elevated Privilege</li> <li>• Template for Approval</li> </ul> In addition, you can create custom templates if you choose. Contact Bit9 Technical Support for assistance in custom template implementation.
<b>Criteria: File Activity and Prevalance alerts</b>	<b>Threshold</b>	Threshold of affected computers required to trigger the alert. Appears only if applicable to the alert type. This can be a percentage or an absolute number.
<b>Criteria: File Activity alerts</b>	<b>Time Period</b>	Minimum time period within which activity must occur to trigger the alert. Appears only if applicable to the alert type.
<b>Criteria: Baseline Drift alerts</b>	<b>Drift Report</b>	Name of the drift report whose data you want to analyze to trigger alerts. Appears only if applicable to the alert type.



Section	Field	Description
	<b>Alert When</b>	The drift parameter you want to measure and the threshold at which it triggers an alert. Appears only if applicable to the alert type.
<b>Criteria: File Prevalence alerts</b>	<b>Specify File By</b>	The way you want to identify a file – the choices are <b>Hash</b> and <b>Filename</b> .
	<b>File Name</b>	Filename to monitor for the alert. Appears only if you chose filename for <i>Specify file by</i> . <b>Note:</b> You cannot use wildcards in the file name for a prevalence alert.
	<b>Publisher Contains (optional)</b>	The name of the publisher (if any) identified as the source of the file. Appears only if you chose filename for <i>Specify file by</i> .
	<b>Hash Type</b>	The type of Hash (MD5, SHA-1 or SHA-256) you are using to identify the file. Appears only if you chose Hash for <i>Specify file by</i> .
	<b>Hash Value</b>	The hash value of the file. Appears only if you chose <b>Hash</b> for <i>Specify file by</i> value type.
<b>Criteria: Event Alerts</b>	<b>Threshold</b>	Number of times an event or event rule must match the properties defined in this rule during the specified time period to trigger an alert.
	<b>Time Period</b>	Time period during which the conditions defined in this rule must be met to trigger an alert.
	<b>Trigger On</b>	Specifies whether the alert is triggered by <b>Event(s)</b> or an <b>Event Rule</b> .
	<b>Select Event Properties</b>	If you chose to trigger on Event(s), the properties of the event(s) that will trigger this alert. The properties include: <ul style="list-style-type: none"> <li>• Subtype – A rule set to trigger on events must include at least one subtype, and may contain more than one.</li> <li>• Other properties – The Add filter menu includes other event parameters that may be added to more narrowly specify the conditions under which an alert is triggered.</li> </ul>
	<b>Select File Properties</b>	If you chose to trigger on Event(s), you may optionally add properties that a file mentioned in the event must meet to trigger this alert. It is not necessary to include file properties, but if specified, the alert will not trigger if the property specified does not match the rule or if the value of property is unavailable for the event.

Section	Field	Description
	<b>Select Process Properties</b>	If you chose to trigger on Event(s), you may optionally add properties that the parent process of the file specified in file properties must meet to trigger this alert. It is not necessary to include process properties, but if specified, the alert will not trigger if the property specified does not match the rule or if the value of property is unavailable for the event.
	<b>Event Rule</b>	If you chose to trigger on Event Rule, an Event Rule menu lists the existing rules.
<b>Policies</b> (appears only for appropriate alert types)	<b>Rule Applies To</b>	Click the radio button to activate this alert for <b>All policies</b> or <b>Selected policies</b> . For <i>Selected policies</i> , check the box next to each policy for which you want the alert enabled.
	<b>Selected</b>	Policies that will be subject to this alert. Select policies and use the arrow buttons to move them into the appropriate column.
<b>Subscribers</b>	<b>Email</b>	<b>Note:</b> You cannot add subscribers (the fields do not appear) until after the alert is created. Add all email addresses to which you want alert notifications sent. Enter each address in the <i>Email address</i> box, and click the <b>Add</b> button each time to create a subscriber list. <b>Add</b> is enabled when you enter a qualified email address. The dropdown menu to the right of the address box specifies the format of the notification email. The choices are: <b>text</b> , <b>HTML</b> , or <b>Auto</b> . <b>Auto</b> allows the recipient's mail server to determine the format.
<b>Reminder Mail</b>	<b>Status</b>	Reminder Mail status determines whether alert email is resent after a specified period of time when the alert has <i>not</i> been reset. The choices here are <b>Enabled</b> or <b>Disabled</b> .
	<b>Remind Every</b>	When Reminder Mail is enabled, the amount of time between alert email re-sends for alerts that are not reset.
<b>Auto Reset</b>	<b>Status</b>	Auto Reset determines whether an alert will be reset automatically, either after a specified time period or, for certain alerts, when conditions that triggered the alert are no longer in effect. When this setting is <b>Enabled</b> , alerts may be auto-reset. When this setting is <b>Disabled</b> , alerts must be reset manually.
	<b>Reset After</b>	If Auto Reset is enabled, this setting determines the time period after which a triggered alert instance will auto-reset if it has not already been reset for another reason. The default value is 4 weeks. It may be changed to a different period, ranging from minutes to weeks.

## Informational Tags for Event Alert Messages

The Alert Message can provide additional documentation for you and others about the conditions that triggered an alert. For Event Alerts, you can add tags to the message so that it provides data specific to the alert instance. [Table 76](#) shows the available tags.

**Table 76:** Informational Tags for Event Alert Messages

Tag	Description
<FileName>	Name of the file from the event initiating the alert. If multiple files led to the alert, contains a comma-separated list.
<Sha256>	SHA-256 hash of the file from initiating event. If multiple files led to the alert, contains a comma-separated list.
<Md5>	MD5 hash of the file from the initiating event. If multiple files led to the alert, contains a comma-separated list.
<Sha1>	SHA-1 hash of the file from initiating event. If multiple files led to the alert, contains a comma-separated list.
<RootSha256>	Root SHA-256 hash of the file from the initiating event. If multiple files led to the alert, contains a comma-separated list.
<HostName>	Name of computer from the initiating event. If multiple computers led to the alert, contains a comma-separated list.
<UserName>	Username from initiating event. If multiple users led to the alert, contains a comma-separated list.
<EventRuleName>	If an event rule initiated the alert, the name of the rule.
<EventRuleDescription>	If an event rule initiated the alert, the description of the rule.
<EventSubtype>	The subtype of the initiating event. If multiple events led to the alert, contains a comma-separated list.
<EventDescription>	Description field from the initiating event.
<AntibodyId>	ID of the file from initiating event. If multiple events led to the alert, contains a comma separated list.
<HostId>	ID of the host from the initiating event. If multiple events led to the alert, contains a comma separated list.

## Editing Alerts

You may need to modify an alert to change its threshold, the time period it covers, its subscribers, or some other parameters. In addition, you may need to enable or disable the alert. All of this is done through the Alert Information page.

### To edit, enable or disable an alert:




1. If you are not already on the Alerts page, click **Alerts** in the Bit9 Console menu.
2. Click the View Details button (pencil and file) next to the alert you want to modify. The Alert Information page appears.
3. If you only want to enable or disable the alert, click the appropriate button in the General section of the Alert Information panel and then click the **Save** button at the bottom of the page.
4. If you want to make other changes, edit the appropriate parameters (see [Table 75](#)) and then click **Save**. The alert is updated and you return to the Alerts page.

Although you can't create new instances of built-in alerts, you can edit some of their settings. For example, you can change the number of approval requests necessary to trigger an Approval Request alert. You also can modify which actions (creation, editing, deletion) trigger an Updater Modified alert.

## Alert Priority

Each Bit9 alert is assigned a Priority, which can be High, Medium, or Low. Alert priority determines the icon shape and color used to represent an alert in the console banner and dashboard, and the color of the rows for triggered alerts on the Alerts page.

**Table 77:** Alert Priorities

Alert Priority	Icon	Row Color
High		Red
Medium		Orange
Low		Yellow

In addition to providing a visual cue that one alert is more important than another, alert priorities also allow grouping on the Alerts page, making it easier to give attention to the most important alerts first. When you choose Priority on the Group by menu, alerts are sorted first by Priority and then by Date Triggered, in descending order.

System alerts have predefined priority levels that cannot be changed:

- Database Limit Alert -- High
- Database Verification Alert -- High
- Bit9 SRS Unavailable Alert -- High

For other alerts, you can change priority using the Action menu on the Alerts table page or the Priority menu on the Add/Edit Alert page.

## Deleting Alerts

When you delete an alert, you delete the definition of the alert and end any monitoring you have been doing with it. As an alternative, you can disable an alert if you don't want it to be active but might use it in the future. You cannot delete the some pre-defined alerts provided by the Bit9 Server, and these do not have a Delete button.

### To delete an alert:

1. On the Alerts page, click the Delete (x) button next to the alert you want to delete.
2. On the confirmation dialog box, click **Yes**.

## How Alerts are Triggered

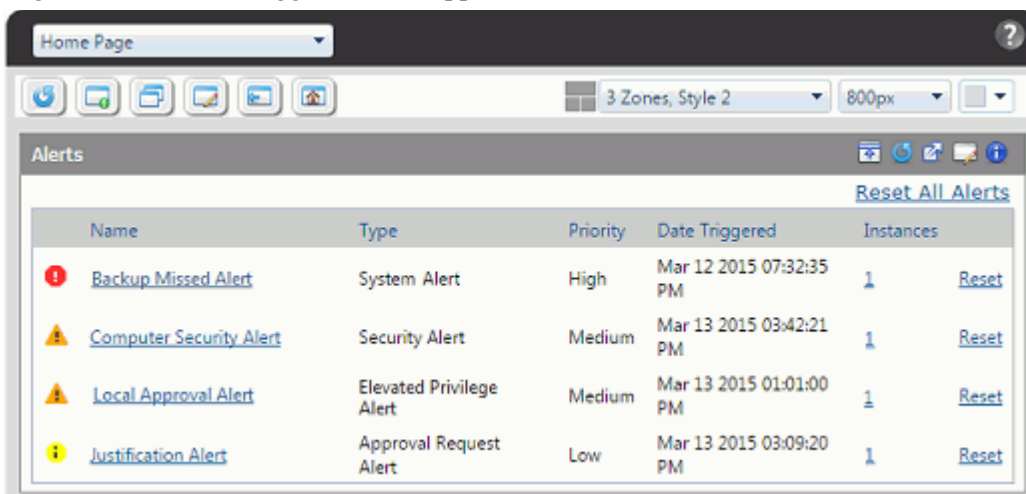
Any alert shown on the Alerts page, whether it was built-in or created by you, can be considered an *alert class*. Each time conditions exist that meet the triggering condition of that alert class, an *alert instance* occurs. For some alert classes, it is only possible to have one instance. For example, there is only one database for a Bit9 Server, and so the Bit9 Database Limit Alert can have only one instance at a time. For other classes, there can be many instances simultaneously. For example, there might be multiple malicious files on a network, and so there could be multiple Malicious File Detected alert instances.

When any triggered instances of an alert class exist, the alert is highlighted on the Alerts page using the color-coded severity level, and a Reset button is added next to the alert name. The Date Triggered column shows when the alert was triggered, and the Instances column shows the number of triggered instances and links to the Alert Instances page. By default, triggered alerts appear at the top of the page, in descending order of when they were triggered.

The console does not display new banners for each alert *instance* during a console login session, but the number of instances is shown. The view below shows triggered alerts without grouping and sorted by Date Triggered.

	Name	Type	Enabled	Priority	Date Triggered	Instances
<input type="checkbox"/>	Local Approval Alert	Elevated Privilege Alert	Yes	Medium	Mar 14 2015 02:36:47 PM	1
<input type="checkbox"/>	Backup Missed Alert	System Alert	Yes	High	Mar 14 2015 02:33:27 PM	1
<input type="checkbox"/>	File Propagation Alert	File Activity Alert	Yes	Medium	Mar 14 2015 02:26:25 PM	1
<input type="checkbox"/>	Approval Request Alert	Approval Request Alert	Yes	Low	Mar 12 2015 07:03:36 AM	1
<input type="checkbox"/>	Updater Modified Alert	System Alert	Yes	Low		
<input type="checkbox"/>	Computer Security Alert	Security Alert	No	Medium		
<input type="checkbox"/>	Justification Alert	Approval Request Alert	No	Low		

In addition, triggered alerts appear on the Alerts portlet, which is on the default Home Page, and a count of triggered alerts appears in the console banner.

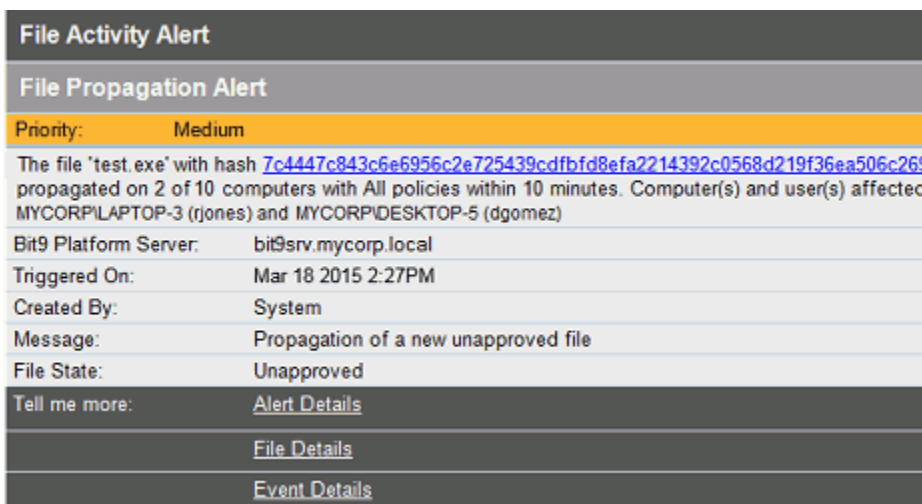


## Mail Notification for Triggered Alerts

When an alert is triggered, notification mail is sent to each subscriber to that particular alert and, if configured, to the global alert subscriber.

While the Bit9 Console shows one banner per triggered alert *class*, the Bit9 Server sends alert email for every *instance*. Instances are defined as distinct cases that match the alert conditions. In the case of malicious files, for example, if the same malicious file shows up 20 times before you reset the alert, it only counts as one instance. But if 20 *different* malicious files appear before the alert notification is reset, each one counts as an instance and each one generates a new email message to alert subscribers.

Mail notifications contain basic information about the alert such as the time of this action for this instance alert, the system(s) on which an action took place, the logged in user, and the file hash. The File Propagation Alert mail shown below is typical of file-related alerts – the exact information provided varies by alert type.



As the example above shows, mail notifications also include links to console pages that display information relevant to the alert, in this case, Alert Details (the list of instances for

this alert), the File Details page for the triggering file, and where relevant, Event Details related to the file (hash) that is the subject of the alert. File and Event Details are not included for non-file alerts. There also may be a Manage Computers link to the Computers table for events that involve Bit9 settings such as the policy for the computer.

Each email generated by a new instance of the same alert class is tracked in the same Alert History and has a link to that instances of that alert. When you reset an alert, the instance history is cleared, but a record of when it was first triggered during this session remains. See [“Viewing Alert Instances and History”](#) on page 510 for an example of the history and instance list for one triggered alert.

### Note

The details provided in an alert notification email describe a particular *instance* of the alert. When you click the Alert Details link in email, it opens the Alert Instances page, which shows the details for *all* instances of the triggered alert.

## Reminder Mail for Triggered Alerts

If you enable Reminder Mail for an alert, a new email notification of that alert is generated on a schedule you specify as long as the alert has not been reset (manually or automatically). For example, if a Bit9 SRS Unavailable Alert is triggered, email is sent immediately. If Reminder Mail is not enabled, no subsequent email will be sent about this alert unless it is reset and then the condition reappears.

If Reminder Mail *is* enabled, and is set for 30 minutes, subscribers to this alert receive a new email about it every 30 minutes until connectivity is restored or the alert is reset.

## Manual and Automatic Alert Resets

Resetting an alert means taking it out of the "triggered" state and clearing the history of all the current instances that caused it to be triggered in the first place. When an alert is reset, it no longer appears on the Triggered Alerts portlet or as a highlighted item on the Alerts page. If the conditions that match the alert return, a new alert will be triggered, new email will be sent to subscribers, and the alert will appear in the usual places in the console.

An alert may be reset manually or automatically:

- **Manual reset** - You manually reset an alert by clicking the alert's Reset button on the Triggered Alerts portlet, the Alerts page, or the Alert History page. In addition to resetting the alert, this adds a "Reset" event to the alert history, with a time stamp and the account name of the Bit9 Console user doing the reset.
- **Automatic reset due to a time limit** – If Auto Reset is enabled for an alert, a time period can be set for an automatic reset. If the alert has not be reset manually or because of change in conditions by the time this time period expires, it will be automatically reset. The default value is 4 weeks. If you want to allow automatic resets for changes in alert conditions but do not want an alert to auto reset based on time, you can use a very large number of weeks as the value in this field. A time-based automatic reset adds an "Auto-Reset" event to its history, with a time stamp. Automatic resets do not cause alert email to be sent.
- **Automatic reset due to changed conditions** – If Auto Reset is enabled for an alert, changes in the conditions that triggered the alert may automatically reset the alert. If


the conditions that trigger an alert instance no longer exist, that instance is removed from the list of triggered instances for the alert class it is in. If *no* triggered instances currently exist for an alert class, the alert notification is reset automatically. The conditions that trigger resets differ from one alert type to another, and some types do not auto reset in this way (although they still can auto reset by time period). An automatic reset of an alert adds an “Auto-Reset” event to its history, with a time stamp and user making the change listed. However, automatic resets do not cause alert email to be sent.

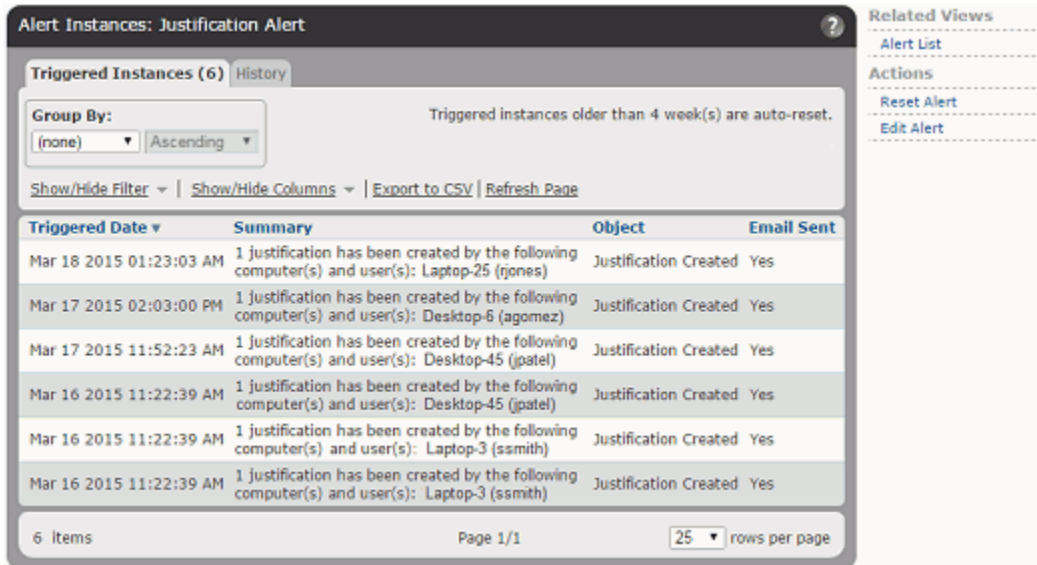


**Table 78:** Reset Conditions for Different Alert Types

Alert Type	Reset Condition
<b>Backup Missed Alert</b>	Resets when backup is successful
<b>Database Limit Reached</b>	Resets when database size falls below the threshold
<b>Database Verification Failed</b>	Resets when database verification succeeds
<b>Potential Risk or Malicious File Detected</b>	Resets when <i>none</i> of the files that triggered the alert (or would have if they had been detected first) are present
<b>Bit9 SRS Unavailable Alert</b>	Resets when your Bit9 Server successfully reconnects to Bit9 SRS and synchronization of Bit9 SRS data with the server is operating properly. This generates an event.
<b>Local Approval Alert</b>	Resets when no machines are in Local Approval mode
<b>File Prevalence</b>	Resets if the prevalence of the specified file falls below the specified threshold
<b>Baseline Drift</b>	Resets when the drift in the specified drift report falls below the specified threshold for the specified parameter (user, computer, or policy)
<b>Computer Security</b>	Resets when the conditions leading to it are no longer met (if this change is detectable).
<b>Approval Request Alert</b>	Resets if enough approval requests are Closed that the total number in Submitted or Open state goes below the triggering threshold.
<b>Justification Alert</b>	Resets if enough justifications are Closed that the total number in Submitted or Open state goes below the triggering threshold.
<b>File Propagation and Block Propagation Alerts</b>	No conditional reset because they are time-based alerts. For example, if an alert determined that a particular file propagated to 20 percent of your machines in a one hour period, no future event can change what happened during the one hour period in the past, so the alert remains triggered. Automatic reset by Auto Reset time period only
<b>Updater Modified Alert</b>	No conditional reset because once an updater is modified it remains modified. Automatic reset by Auto Reset time period only
<b>New Certificate Alert</b>	No conditional reset. Automatic reset by Auto Reset time period only.
<b>Revoked Certificate Alert</b>	No conditional reset. Automatic reset by Auto Reset time period only.
<b>Event Alert</b>	No conditional reset. Automatic reset by Auto Reset time period only.
<b>System Health OER Alert</b>	Resets when no OER indicators on the System Health page show an issue.

## Viewing Alert Instances and History

If an alert is currently triggered, you can view the instances that triggered it by clicking its View Instances button (  ) on the Alerts page. The Alert Instances page shows the date, summary explanation, the object of the alert (what it was and the action taken, such as created, modified, deleted, etc.), and whether email was sent for each instance.



Alert Instances: Justification Alert

Triggered Instances (6) History

Group By: (none) Ascending

Triggered instances older than 4 week(s) are auto-reset.

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page


Triggered Date	Summary	Object	Email Sent
Mar 18 2015 01:23:03 AM	1 justification has been created by the following computer(s) and user(s): Laptop-25 (rjones)	Justification Created	Yes
Mar 17 2015 02:03:00 PM	1 justification has been created by the following computer(s) and user(s): Desktop-6 (agomez)	Justification Created	Yes
Mar 17 2015 11:52:23 AM	1 justification has been created by the following computer(s) and user(s): Desktop-45 (jpatel)	Justification Created	Yes
Mar 16 2015 11:22:39 AM	1 justification has been created by the following computer(s) and user(s): Desktop-45 (jpatel)	Justification Created	Yes
Mar 16 2015 11:22:39 AM	1 justification has been created by the following computer(s) and user(s): Laptop-3 (ssmith)	Justification Created	Yes
Mar 16 2015 11:22:39 AM	1 justification has been created by the following computer(s) and user(s): Laptop-3 (ssmith)	Justification Created	Yes

6 Items Page 1/1 25 rows per page

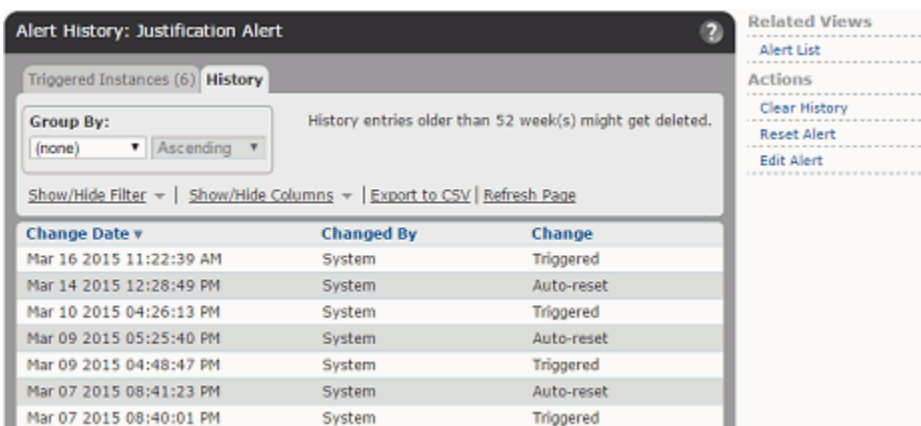
Related Views: Alert List

Actions: Reset Alert, Edit Alert

When an alert is reset, details of the instances that triggered it are deleted.

You can view the history of any alert by clicking its View Instances button (  ) on the Alerts page and clicking on the **History** tab, or clicking that tab from the Alert Instances page. If the alert is not triggered, the History tab is the only tab available when you click on the View Instances button.

The Alert Instances History page includes information about when the alert was created and modified (and by whom), when it was triggered and reset, subscriber additions, and if it was enabled or disabled.



Alert History: Justification Alert

Triggered Instances (6) History

Group By: (none) Ascending

History entries older than 52 week(s) might get deleted.

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Change Date	Changed By	Change
Mar 16 2015 11:22:39 AM	System	Triggered
Mar 14 2015 12:28:49 PM	System	Auto-reset
Mar 10 2015 04:26:13 PM	System	Triggered
Mar 09 2015 05:25:40 PM	System	Auto-reset
Mar 09 2015 04:48:47 PM	System	Triggered
Mar 07 2015 08:41:23 PM	System	Auto-reset
Mar 07 2015 08:40:01 PM	System	Triggered

Related Views: Alert List

Actions: Clear History, Reset Alert, Edit Alert

Both the Alert Instances and the Alert History views have menus for taking actions on alerts, and most of the commands on these menus appear for both tabs:

- **Alert List** – Returns to the Alerts table page.
- **Clear History** – (History page only) Clears all of the history for this alert.
- **Reset Alert** – (Triggered alerts only) Resets the alert from its triggered state and deletes the current instances.
- **Delete Alert** – (Only if alert can be deleted) Deletes the alert itself from the list of available alerts.
- **Edit Alert** – Opens the Edit Alert page so you can modify the configuration of the alert.

### Important

**Reset Alert** eliminates the detailed history of *instances* between the most recent triggering of the alert and the last time you reset it, but leaves all other information in place, including the date and time that the alert was triggered.

**Clear History** deletes *all* of the alert’s history, including information about its creation, modification, subscribers, and all triggering and reset events. Be sure you do not need this information before clearing the alert history.

## Managing Alert Email Subscriptions

There are two types of subscriptions for alerts email:

- **For specific alerts** – On the Alert Information page, you can add subscribers to the email notifications specific to that alert.
- **For all alerts** – On the System Configuration page, you can set up *one* global subscriber for alerts email. See [“Specifying a Global Alert Subscriber”](#) on page 639.

### Important

Subscribers receive alert email only if alerts email is properly configured and enabled on the System Configuration page. See [“Configuring Alert and Approval Request Mail”](#) in the “Bit9 Configuration” chapter for more information.

Subscription to individual alerts is the normal means of setting up email notification. This allows you to decide which alerts are of interest to a particular user and avoid burying them in other alert email. Users can always watch the Triggered Alerts portlet or the Alerts page for alerts not critical enough to require email notification.

#### To add a subscriber to the email notification list for one alert:

1. On the Alerts page, click the View Details (pencil and file) next to the alert you want to modify.
2. On the Alert Information page, scroll down to the Subscribers panel, click in the **Email Address** text box, and paste or type the subscriber name.

3. Choose the email type (**Auto**, **Text**, or **HTML**) from the dropdown menu. The default is Auto, which allows the server to determine the best format for the recipient based on information about the recipient's email system.
4. Click **Add** to add the subscriber. The new subscriber name appears in the list below the subscriber entry line.
5. Add any other subscribers you want to receive notifications when this alert is triggered.
6. Click **Save** at the bottom of the Alert Information page. The new subscribers are added to the distribution list for this alert.

You can edit the email address or delivery format of existing subscribers by opening the Alert Information page as you did to add the subscriber and then clicking **Edit** next to the subscriber name. When you have finished editing the subscriber information, click **Update** next to the name, and then click **Save** at the bottom of the Alert Information page. *Be sure to click both buttons.*

You can delete a subscriber from the email notification list for an alert by opening the Alert Information page and clicking **Remove** next to the name. Note that there is no confirmation for this action – the name is removed immediately.

## Detecting Agent Issues with Computer Security Alerts

Although many Bit9 alerts are related to computer security, there is one built-in alert that is specifically designed for this purpose. The Computer Security Alert, which is disabled by default, is triggered by events that may indicate suspicious behavior.

The screenshot shows the 'Edit Alert' window for the 'Computer Security Alert'. The window is divided into three sections: General, Type, and Criteria. In the General section, the Alert Name is 'Computer Security Alert', the Message is 'Suspicious behavior detected', the Priority is 'Medium', and the Status is 'Enabled'. In the Type section, the Type is 'Security Alert', the Description is 'Alerts subscribers when a suspicious behavior is detected', and the Mail Template is 'Default'. In the Criteria section, the Alert When field has four checked options: 'Computer not protected', 'Agent tampering detected', 'Agent tampering prevented', and 'Computer clock out of sync'.

### Criteria Triggering a Security Alert

There are four triggering criteria that can be enabled in the Computer Security Alert - by default, all are enabled when you enable the alert itself. Which one of these criteria triggers a security alert is identified in Summary field on the Alert Instance page, and in the email notification (if enabled) sent due to the alert.

The criteria for triggering a Security Alert are:

- **Computer not protected** – This condition occurs if an agent upgrade fails. It means that the Bit9 Agent is not running on the identified computer, and so the computer is not protected by Bit9 (the Connection status indicator for this computer on the Computers page will be red). Restoring the agent to proper operation automatically resets the alert when this is the triggering condition.
- **Agent tampering detected** – If Bit9 Agent tamper protection is accidentally disabled through the Bit9 Console and a user on a computer running the Bit9 Agent modifies the agent folder (for example, by adding a new file), the Computer Security Alert is triggered with the summary description "Agent tampering detected". As soon as an administrator re-enables the tamper protection for the Bit9 Agent, this alert is automatically reset.
- **Agent tampering prevented** – If a user on an agent-managed computer attempts to tamper with the agent and fails, the Computer Security Alert is triggered with the summary description "Agent tampering prevented". An example of this might be a user attempting to copy files to the agent folder (Bit9\Parity Agent) but failing because of tamper protection. Another example might be unauthorized attempts to run special agent management commands (i.e., without a correct password). When this condition triggers the alert, the alert must be reset manually.
- **Computer clock out of sync** – One way to attempt to run malware or other unauthorized files without detection is to change the clock on the targeted system to create an invalid timestamp. The Bit9 Agent still detects and reports a file execution under these circumstances, but generates a Computer Security Alert with the summary description "Computer clock out of sync" as soon as the discrepancy between the Bit9 Server clock and the agent clock is detected. Correcting the system time on the computer that is the source of the unauthorized activity will allow this alert to be reset by the next event received by the Bit9 Server.

When a Computer Security Alert is enabled, *any* of the enabled criteria on any computer will trigger it. While the alert is triggered, additional cases of the triggering condition on the same computer are recorded in the history, but do not create another alert instance. If the same computer reports an event that meets a *different* triggering condition, however, another instance is displayed. For example, two failed attempts at tampering do not create two alert instances unless the alert is reset between them. However, an attempt to tamper followed by a clock out of sync on the same computer does create two different alert instances.

As with all alerts, each instance results in an email notification, if notification is enabled and properly configured. Both the Alert Instance displayed in the Bit9 Console and the email notification of the alert contain the security event description, the name of the computer on which it happened, and the time of triggered instance.

#### Note

Because the Computer Security Alert is based on Bit9 Agent events, a disconnected agent will not produce an alert when the triggering conditions are met. In addition, in environments with a large number of agents, files and changes, this alert might be delayed if a large number of events is being processed by the Bit9 Server when the agent reports the security events.

## Alerts for File Prevalence

On the File Catalog tab of the Files page, there is a *Prevalence* column that shows you how many computers a file is on (based on periodic updates).

The screenshot shows the 'Files: All Unique Files' interface. It includes a 'File Catalog' tab, 'Saved Views' (currently '(none)'), 'Group By' (currently '(none) Ascending'), and 'Max Age' (currently 'None'). Below these are controls for 'Show/Hide Filter', 'Show/Hide Columns', 'Show/Hide Snapshot', 'Export to CSV', and 'Refresh Page'. The main table has columns: Action, First Seen Date, First Seen Name, Publisher or Company, Prevalence, Trust, and Global State. The 'Prevalence' column is highlighted with a red box.

Action	First Seen Date	First Seen Name	Publisher or Company	Prevalence	Trust	Global State
	Nov 29 2013 10:00:25AM	googleupdatesetup.exe	Google Inc.	54	10	Approved
	Nov 20 2013 04:56:34PM	solsuite.exe	TreeCardGames.com	35	8	Unapproved
	Nov 19 2013 11:03:24AM	crashreporter.exe	Mozilla Corporation	23	10	Approved
	Nov 19 2013 11:03:24AM	brwsrcomp.dll	Mozilla Corporation	23	10	Approved
	Nov 16 2013 09:14:48AM	swdir.dll	Adobe Systems Incorporated	5	10	Approved

When Prevalence is listed in a table, you can sort the table by prevalence or set Filters on the page to show a report of only those files with a prevalence greater than or equal to a number you specify. If a file was seen by an agent and reported to this Bit9 Server at one time but now has a prevalence of zero, it is removed from the table, although you can view it by choosing **Removed Files** from the Saved Views on the Files page.

## Prevalence Alerts

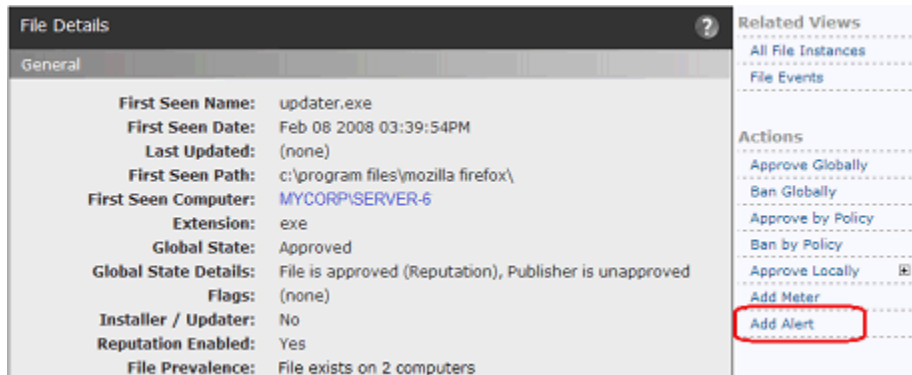
Prevalence alerts are triggered when the prevalence of a particular file reaches a threshold you set. You can go to the Alerts page and type in information about the file you want to create an alert for, but the easiest way to create a prevalence alert is from the File Details page of the file you want to track. See [“Using Bit9 Alerts”](#) on page 494 for more information about alerts.

### Notes

- You cannot use wildcards in the filename for a prevalence alert.
- Provide a name, not a path, for prevalence alerts.

**To create a prevalence alert for a file from its File Details page:**

1. On the Files page, click on the View Details (pencil and file) button next to the name of the file whose propagation you want to track. The File Details page opens.



2. On the File Details page for that file, click **Add Alert** in the Actions menu. The Alert Information page opens with the name of the file and its hash automatically filled in.

The screenshot shows the 'Add Alert' dialog box. The 'General' tab is active, and the 'Alert Name' is 'Prevalence of updater.exe'. The 'Message' field contains the text: 'File updater.exe is present on more than specified number of computers.'. The 'Priority' is set to 'Medium' and the 'Status' is 'Enabled'. The 'Type' is 'File Prevalence Alert'. The 'Criteria' section shows 'Specify File By' set to 'Hash', 'Hash Type' as 'SHA-256', 'Hash Value' as '0ff923cf6b8883f79e7f3220270a9cf3e6270ad915680774f3f2d6ed327b0e3b', and 'Threshold' as '10'. The 'Subscribers' section has a note: 'Alert must be created before email recipients can be specified'. The 'Reminder Mail' section has 'Status' set to 'Disabled' and 'Remind Every' set to '1 day(s)'. The 'Auto Reset' section has 'Status' set to 'Enabled' and 'Reset After' set to '4 week(s)'. At the bottom, there are buttons for 'Create & Exit', 'Create', and 'Cancel'.

3. Set the remaining parameters you want for this alert including:
  - a. Threshold number of computers on which this file must appear to trigger the alert.
  - b. Reminder mail specifications if you want periodic email reminders to be resent after a certain period of time if the alert is not reset or the condition not remedied.
4. Click **Create**, if you want to stay on this page or **Create & Exit** to go to the Alerts table page. You now have a prevalence alert for this file, visible on the Alerts page.
5. To add email alert subscribers, click the View Details (pencil and file) button for the alert and add the addresses in the Subscribers section of the Alert Information page.

## Monitoring Specific File Executions

Software metering enables you to track the number of times users run specified files. When you create a meter, you specify a file to be tracked. Each time the specified file runs on a computer, the server records its execution. Configurable reports enable you to display cumulative execution events by time of execution, user, computer, and policy. You can create as many meters as you need and centrally manage them (view reports, edit, and delete) in one place. Monitoring begins almost immediately after you create the meter.

Software metering is useful for the following purposes:

- Gathering data about how often applications are used
- Determining which computers are running an application
- Locating computers running older versions of software for upgrade or completely retiring obsolete applications

### Notes

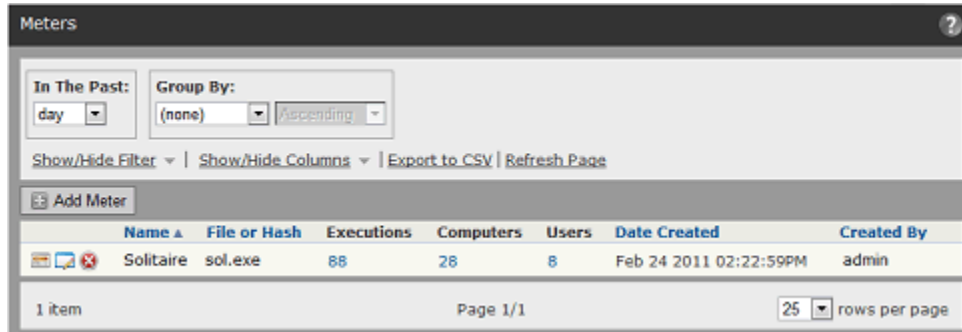
- Bit9 Agent is one of the first processes to start when you start your computer. It is normally configured so that a user cannot log in to an agent-managed computer until the agent has started up, or a specified timeout period expires. However, if a service or process is configured to start before the agent, its activity is not monitored or controlled until the agent starts.
- You can locate *all* executed files on your network, or on a subset of your computers, using Filters on the Find Files page or the Files on Computers tab on the Files page. See [Defining a Search on the Find Files Page](#).

You can create a meter from scratch, as shown in the procedure immediately below, or you can create a meter for a file directly from its File Details page – see [“Creating a Meter from the File Details Page”](#) on page 520.

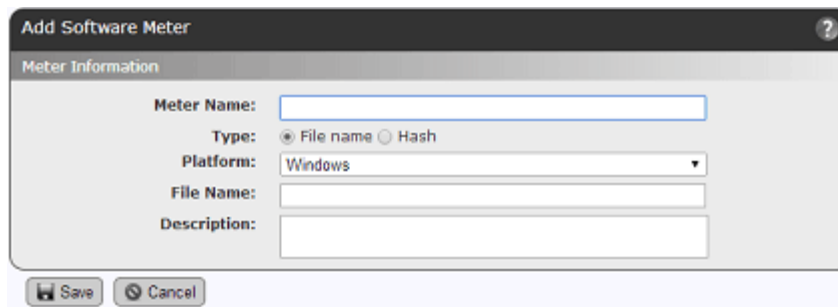


**To meter execution of specified file(s):**

1. On the console menu, choose **Tools > Meters**. The Meters page appears:



2. On the Meters page, click **Add Meter**.



3. On the Add Software Meter page, select the type of identification (file name or hash) you want to use for this file. Additional fields appropriate for the selected type appear.
4. In the Software Meter panel, specify information about the file to be monitored.

**Table 79:** Software Meter Parameters

Field	Description
<b>Meter name</b>	Text description of the software to be metered.
<b>Type</b>	To meter a file you must know the name of the file or its hash (data signature). Choose either one, as appropriate. Note that File Name meters are platform-specific; hash meters apply to all platforms. A meter created directly from a File Details page automatically has that file's SHA-256 Hash (if available) entered as the file identifier.
<b>Platform</b>	For file name meters, the platform (Windows, Mac, or Linux) for which the meter is in effect. File name meters can be used for one platform only. (Field does not appear for hash meters.)

Field	Description
<b>File Name</b>	<p>File name (or path) to which this meter applies. If you provide just a file name, execution of that file in any location is metered. If you provide a path that ends in a file name, only executions of the file in the specified location are metered.</p> <p>If the path you enter ends with a directory, the meter counts all executions in that directory and all of its subdirectories.</p> <p><b>Platform Notes:</b></p> <ul style="list-style-type: none"> <li>For Windows paths, you can specify a local drive name (for example, C:\dir\subdir\application) or a UNC path (for example, \\dir\subdir\application). You cannot specify mapped drives (for example, Z:\application) for network access.</li> <li>For all paths, you must use the correct directory delimiters for the platform you choose.</li> <li>You can switch platforms after a meter is created, but keep in mind platform differences, such as directory delimiters and drive letters, that might make a path invalid on a different platform.</li> </ul>
<b>Hash Type</b>	<p>Cipher algorithm used to create the hash you want to monitor (MD5, SHA-1, or SHA-256). Note that Bit9 returns SHA-256 hashes by default for Files or Find Files searches, but cross-references it so you can monitor, approve or ban by the other hash types. If you create a meter directly from a File Details page, that file's SHA-256 Hash (if available) is used as the file identifier.</p>
<b>Hash Value</b>	<p>Hash (data signature) for the file.</p> <p>Monitors file execution on computers even if the hash has been previously identified. If you enter a hash from an external source, computers running the Bit9 Agent register its execution upon first encounter.</p> <p>To locate hashes on your network, use the Files page or Find Files utilities. Note that you can create a meter directly from the File Details page for any file identified on the Bit9 Server.</p>
<b>Description</b>	<p>Optional text that further describes the metered file. To display this information, add the Description column to the Meters table.</p>

For example, a meter to monitor executions of Microsoft Excel by its name might be specified as shown in the screen below:

The screenshot shows a dialog box titled "Add Software Meter" with a question mark icon in the top right corner. Below the title bar is a section labeled "Meter Information". The form contains the following fields:

- Meter Name:** Microsoft Excel
- Type:**  File name  Hash
- Platform:** Windows (dropdown menu)
- File Name:** excel.exe
- Description:** Keep track of the number of times Excel is started up. (text area)

At the bottom of the dialog are two buttons: "Save" and "Cancel".

- To add the file to the table of metered files, click **Save**. The meter is created and activated, and the name of the meter, the metered file, and execution information appears in the Meters table on the Software Meters page:

The screenshot shows the 'Meters' window with the following controls and data:

**In The Past:** day  
**Group By:** (none) Ascending

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Add Meter

Name	File or Hash	Executions	Computers	Users	Date Created	Created By
Solitaire	sol.exe	88	28	8	Feb 24 2011 02:22:59PM	admin
Excel	excel.exe	135	52	46	Jan 10 2012 12:03:34PM	admin

2 items Page 1/1 25 rows per page

- To change meter information, click the View Details button (pencil and file) next to the meter name.
- To display a report of meter events, click the View Report button to the far left of the report name.

### Note

By default, meter events are grouped by computer. To view all executions of files on that computer, expand the computer name. Alternatively, you can eliminate the grouping by choosing **None** on the *Group by* menu.

The screenshot shows the 'Report Parameters' dialog box with the following settings:

**Basic**

Meter Name: Excel  
 File Name: excel.exe

**Time Range**

Ever  In the past...  During range

Past: 1 day(s)

Apply Back

The screenshot shows the 'Meter Report Details' window with the following controls and data:

**Group By:** Computer Ascending

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Timestamp	User	Computer	Policy
Computer: MYCORP\LAPTOP- 1 1 item			
Computer: MYCORP\DESKTOP- 4 2 items			
Jul 24 2012 01:56:31PM	MYCORP\rjones	MYCORP\Desktop-4	Administration
Jul 24 2012 08:28:27AM	MYCORP\rjones	MYCORP\Desktop-4	Administration
Computer: MYCORP\DESKTOP- 6 2 items			
Computer: MYCORP\LAPTOP- 5 3 items			
Computer: MYCORP\LAPTOP- 3 1 item			

- To delete a meter, click the Delete (x) icon next to its name on the Meters page.

## Creating a Meter from the File Details Page

If you know you want to monitor executions of one specific file, you can create a meter directly from its File Details page. This has the advantage of pre-configuring most of the information required for the meter, including the hash value – meters created in this way are automatically Hash type meters.

### To create a software execution meter from a File Details page:

1. Open the File Details page for the file you want to meter.
2. In the Actions menu to the right of the File Details page, click **Add Meter**. The Add Software Meter page appears, with the Hash value of the file already entered and the file name as the default meter name.
3. If you choose, change the Meter name and add a description.
4. Click **Save** to save and enable the meter.

## Chapter 19

## Monitoring Change: Baseline Drift Reports

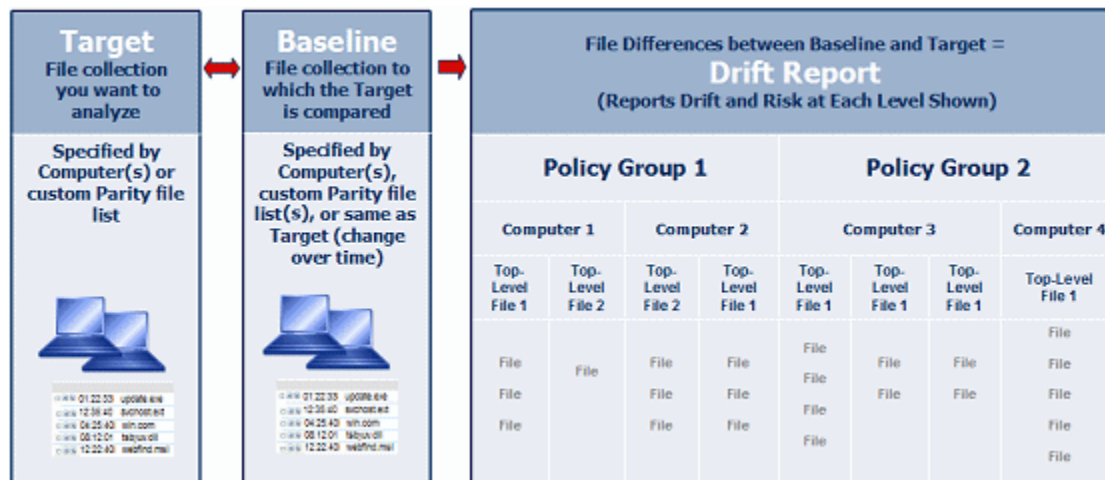
This chapter explains how to use Baseline Drift Reports, which allow you to track changes in the inventory of files on systems running the Bit9 Agent. [Chapter 18, “Events, Alerts and Meters,”](#) describes other monitoring features.

### Sections

Topic	Page
<a href="#">Baseline Drift Overview</a>	522
<a href="#">Viewing and Managing Baseline Drift Reports</a>	524
<a href="#">Responding to Drift Report Results</a>	530
<a href="#">Creating and Editing Reports</a>	532
<a href="#">Drift in Multi-Platform Environments</a>	538
<a href="#">Managing Snapshots</a>	539
<a href="#">Displaying Baseline Drift Reports in Graphs</a>	542
<a href="#">Creating Baseline Drift Alerts</a>	544

## Baseline Drift Overview

Bit9's Live Inventory of files on computers reporting to your Bit9 Server gives you the ability to measure baseline drift, the difference between a baseline of files and the current files on a target you specify. This difference is available as a baseline drift report that you can view either in detail in dynamic tables or as graphic charts on a Bit9 dashboard. Baseline drift reports provide not only simple numbers of file differences but also risk analyses related to those changes.



Once it is set up, a drift report runs automatically every few hours, giving you an up-to-date record of changes in your file inventory. You can create different baseline drift reports for different targets and baselines, and Bit9 provides some reports pre-configured for your use. By default, only Power Users and Administrators can create, modify and delete reports. However, custom account groups can be configured to allow viewing only or viewing and management of drift reports and snapshots.

**Table 80:** Baseline Drift Terminology

Term	Description
<b>Target</b>	A collection of current files that you want to analyze. This might be all the files on a particular computer, on computers with a particular security policy, or on all computers. It also can be a custom filtered table of files from one or more computers.
<b>Baseline</b>	The reference against which you compare the target. It can be a set of files captured as a "snapshot," multiple snapshots, a set of one or more computers, or a custom baseline generated by filters and other parameters you define. You also can have no baseline, in which case a report shows you new files appearing over time.
<b>Snapshot</b>	A set of files collected from one or more computers. It can be <i>all</i> files from the selected computer(s), files selected based on custom-defined filter, or file lists captured from other pages in the Bit9 Console. Each snapshot is named, and can be used as the baseline for a drift report.

Term	Description
<b>Baseline drift report</b>	A report that contains information about the differences between a baseline and a target. A drift report can show differences simply in terms of number of changed files as well as in terms of the risk indicated by those changes.

## How Drift and Risk are Measured

For the designated target, baseline drift reports can provide several different types of data about the computers or files in the report. [Table 81, “Basic Drift Values”](#) describes this information.

**Table 81:** Basic Drift Values

Term	Description
<b>Drift</b>	The amount of drift measured simply in terms of files added, changed, and (if configured for a report) deleted in the target. Files are identified by their hash value. An added file, a changed file, or a modified file each have a drift value of 1. See <a href="#">“Advanced Baseline Drift Report Options”</a> on page 535 for more on how Bit9 determines whether a file has been modified.
<b>Weighted drift</b>	A calculation based on the drift value and adjusted by several factors that might increase or decrease the significance of the drift for each file. Among the adjustment factors are trust level, threat level, file type and associations with other files. For example, the weighted drift for files that have valid digital signatures, have high trust, or were installed by files with high trust will be reduced from what it would be without these factors.
<b>Risk</b>	A calculation similar to weighted drift, but adjusted so that files believed to pose no threat show a risk of zero.
<b>% Weighted drift</b>	The percentage of total weighted drift in the current report contributed by the item in a row.
<b>% Risk</b>	The percentage of total risk in the current report contributed by the item in a row.

Other key factors in determining the total drift and risk reported in a baseline drift report are:

- **File Filtering:** You can decide which files in the baseline and in the target participate in the comparison. For example, the pre-configured drift reports compare Unapproved files, but ignore Banned or Approved files – you can change this if you choose. There are several other file categories you can include or exclude from the comparison. See the [“Using Filters in Target and Baseline Definitions”](#) and [“Advanced Options: File Filter Options”](#) sections below for more detail.
- **File Comparison Method:** By default, if a file hash found in the baseline is also found *anywhere* in the target, it is considered a matching file, and no drift is reported. This is called the *File Content* method. The alternative is the *File Location* method, in

which the same hash in different locations in the baseline and the target is considered a drift. See [“Advanced Options: File Comparison Method”](#) for more detail.

## Viewing and Managing Baseline Drift Reports

All baseline drift reports appear on the Manage Baseline Drift Reports page. Two pre-configured baseline drift reports appear in the console: Drift of all computers, and Daily drift of all computers. These are disabled by default. These pre-configured reports provide a useful way to view the configuration options for baseline drift and view their results in a report. You can copy any existing report and use it as a starting point for new reports.

### To view the table of Baseline Drift Reports:

- On the console menu, choose **Reports > Baseline Drift**.  
The Manage Baseline Drift Reports page appears.

Baseline Drift: Manage Baseline Drift Reports

Reports | Snapshots

Group By:  
(none) | Ascending

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page

Add Report





Action	Name	Date Created	Created By	Date Last Completed	Status
	Drift of all computers	Aug 05 2009 08:12:50AM	System	Jan 08 2012 03:32:37PM	Available
	Daily drift of all computers	Aug 05 2009 08:12:50AM	System	Jan 08 2012 03:29:56PM	Available

2 items Page 1/1 25 rows per page

The Manage Baseline Drift Reports page gives you access to the existing reports as well as the ability to create a new report. On the Manage Baseline Drift Reports page, you can use any of the standard buttons and tools available on a console table page, including filtering, adding or removing columns, and grouping the items in the table. The following table describes the buttons, columns, and tabs on the drift page.



**Table 82:** Manage Baseline Drift Reports Page parameters

Item	Description
<b>Reports and Snapshots</b> tabs	The Reports tab (default) shows the table of all available drift reports and key information about them. It also provides an Add Report button for creating new reports. The Snapshots tab shows the table of all available snapshots and key information about them. See <a href="#">“Managing Snapshots”</a> for more information.
<b>Add Report</b> button	Opens the Add Baseline Drift Report page, on which you can enter the details for a new Baseline Drift Report.
 View Report Results button	Shows the most recent results of the report in its row.
 View Details button	Opens the Baseline Drift Report Details page for the report in its row. You can view and edit the report details on this page.
 Schedule Run button	Schedules the report in its row to be run as soon as possible rather than waiting for the normal report period.
 Delete button	Deletes the report in its row.
<b>Name</b> field	The name of the report. Clicking this name shows the most recent results of the report.
<b>Date Created</b> field	The date and time this report was created.
<b>Created by</b> field	The console user who created this report – reports showing System in the <i>Created by</i> field were provided by Bit9.
<b>Date Last Completed</b> field	The date and time the report was last run. If blank, the report is either disabled or is new and has not completed its first run.
<b>Status</b> field	Shows the current status of the report. The possible values are: <ul style="list-style-type: none"> <li>• <b>Available</b> – Updated report is ready and available for viewing</li> <li>• <b>Available (Updating)</b> – New report is currently being generated. Previous report will be available for viewing until current report generation completes.</li> <li>• <b>Disabled</b> – Report is disabled and is not generating results. Last generated results are deleted.</li> <li>• <b>Not available</b> – Report is new; results have not been generated yet.</li> </ul>

## Viewing Baseline Drift Report Results

If a report listed on the Manage Baseline Drift Reports page shows that it is *Available*, you can view the most recent report results.

### To view a baseline drift report:

1. On the console menu, choose **Reports > Baseline Drift**.
2. On the Baseline Drift page, click the name of the report you want to see in the Manage Baseline Drift Reports table. By default, the initial view shows drift by computer.

## Report Results: Computer View

The figure below shows the initial view of the built-in *Drift of all computers* report. The results show a table of all computers that have had agent-tracked files added or modified in the past 24 hours (deleted files are not tracked by default), and the amount of drift contributed by each computer. Note that the View Mode panel has Computers selected.

Computer	Drift	Risk	Policy
MYCORP\LAPTOP-3	29116	83495.6	IT Group
MYCORP\LAPTOP-1	18693	38537.1	Engineering1
MYCORP\DESKTOP-2	14143	43266.6	Engineering2
MYCORP\LAPTOP-5	6664	12096.8	Testing Group
MYCORP\DESKTOP-7	6508	20559.5	General Admin

## Report Results: File Views

Files views of Baseline Drift Reports provide more detail than Computers views since the key elements of drift are based on the files themselves. There are three primary File views available for drift reports:

- **All Top-level Files** – This is the main Files View of the drift report you choose. It shows the drift, risk, and other data for each top-level file in the report.
- **Files Associated with One Top-Level File** – This is a drift report for the files associated with one top-level file. You can view an associated files report by clicking on a highlighted name in the Top-Level Files report.
- **Files on One Computer** – This is a drift report for all the files on one computer that contribute to drift. You can view a computer-specific files report by clicking on the name of a computer in the Computer view.

In addition to the primary views, there are pre-configured **Saved Views** that give you a different perspective on the information in drift-by-files tables:




- **Drift Contributing to Risk** – This shows the standard report on drift by (top-level) files, except that files with drift risk of 0 are filtered out.
- **Drift by Category** – This view is the equivalent of choosing *Category* in the Group by menu or Filters list. It shows a list of file categories, as reported by Bit9 Software Reputation Service (SRS), in the left column of the table. Clicking on the plus sign next to a category expands the view to include all files in that category and the Drift and Risk levels for each file.
- **Drift by Publisher/Company** – This view is the equivalent of choosing Publisher or Company in the Group by menu or Filters list. It shows a list of the identifiable Publisher/Company names for the files in the left column of the table. Clicking on the plus sign next to a Publisher/Company name expands the view to include all files with that Publisher or Company, and the Drift and Risk levels for each file.

- **Drift by Installed Program** – This view is the equivalent of choosing Installed Program in the Group by menu. It shows total drift of all files associated with an installer program.

**Platform Note:** This view is useful only for Windows agents.

The table below shows the controls and default fields on the Files view of a drift report.

**Table 83:** Drift Report Results Elements

Item	Description
 View Report Results button	In Computer View mode, drills down to the Baseline Drift report for the computer in its row.
 View Details button	In Files views, opens the File Instance Details page for the file in its row.
 Find Files button	(In Files views only) Goes to the Find Files page and shows all file instances matching the hash of the file in its row, on all computers.
<b>File Name</b>	Shows the name of a file in the target that is contributing to drift. If the file is highlighted in blue, it is a link, indicating that it is a top-level file with associated files. Clicking on the link drills down to a Baseline Drift report for the files associated with the named top-level file.
<b>Publisher or Company</b>	Shows the publisher (if available) or company (if available and there is no publisher information).
<b>Drift</b>	In Computer View mode, the sum of drift for all drifted files on the computer in this row. In File views, the sum of drift for this file (if it has no associated files) or for files associated with this file (if it is a top-level file). For views with grouped information, the sum of the drift for each instance of the group parameter. Expanding the group shows drift for each member of the group.
<b>Risk</b>	The sum of the risk for all drifted files on the item in this row. See <a href="#">“How Drift and Risk are Measured”</a> on page 523 for more details.
<b>Threat</b>	A threat level for the file in this row based on a weighted analysis of malware threats known to Bit9 SRS. Threat levels are Malicious (red ! icon), Potentially Malicious (yellow ! icon), Unknown (no icon), or Clean (green ✓ icon).
<b>Trust</b>	On a scale of 0-10, the level of trust for the file in this row. Zero is the lowest level of trust and 10 is the highest. Trust is computed from a variety of factors, including file source, publisher, and identification in Bit9 SRS (e.g., is it malware or some other undesirable category of file).
<b>Computer</b>	Shows which computer the file in this row is on. Clicking on the name opens the Computer Details page for that computer.
<b>User Name</b>	User logged into the computer when the installation was started or top-level file was created.

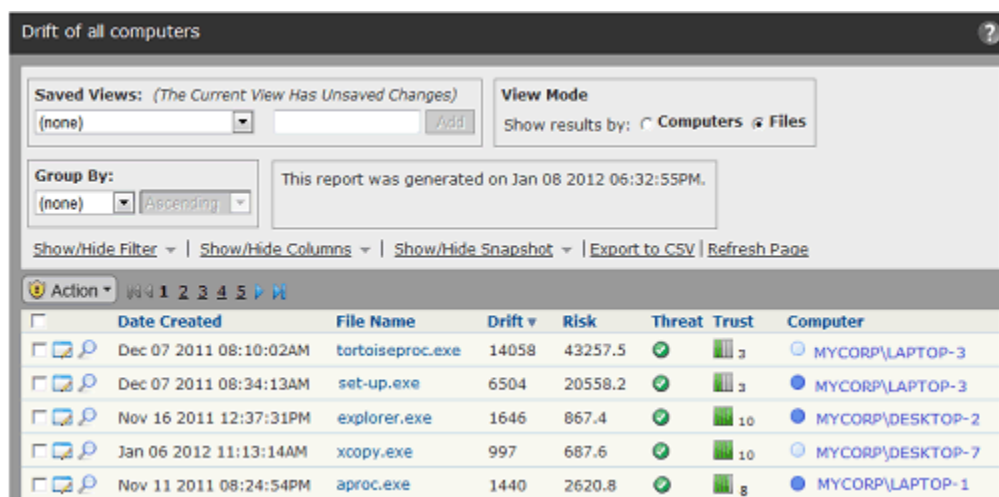
Item	Description
<b>View Mode</b>	Clicking on <b>Files</b> in the View Mode box changes the view from drift by computers to drift by files, and lists the top-level files in the report. Clicking on <b>Computers</b> in the View Mode box changes the view from drift by file to drift by computers, and lists all of the computers in the drift report.  <b>Note:</b> Clicking on <i>Show individual files</i> in the lower right of the table causes the Files view to show both top-level files and any files associated with them.
<b>Saved Views</b>	Files View mode has three saved views. To return to a full list of files in the report, choose <b>none</b> on the Saved Views menu.
<b>Action menu</b>	Allows you to take action on checked files in the drift report. See <a href="#">“Responding to Drift Report Results”</a> on page 530 for details.

## Drift by Files: Top-Level Files on All Computers

The report for top-level files is often the most useful in tracking drift and risk since many of these files are the ones that install other files on computers. They are “top-level” in the sense that they are not generated by other files in the report.

### To display the top-level files view of a baseline drift report:

1. On the console menu, choose **Reports > Baseline Drift**.
2. On the Baseline Drift page, click the name of the report you want to see in the Manage Baseline Drift Reports table.
3. In the View Mode box, click **Files**.  
The top-level Files view appears.



4. If you want the report results to show both top-level files and the files they generate, check the *Show individual files* box in the far right bottom corner of the page.

## Drift by Files: Associated Files Report

A name highlighted in blue indicates that more information is available if you click on the name. On the top-level files report, clicking on a file name gives Baseline Drift Report Results page for files *associated with* the file you clicked. Associated files are files that either were installed by the top-level file or are copies of it (i.e., have the same hash).

Drift of all computers

Saved Views: (none) Add

This report was generated on Jan 08 2012 05:22:55PM

Files associated with 'tortoiseproc.exe' on computer MYCORP\LAPTOP-3 [\[Back to report\]](#)

Group By: (none) Ascending

Show/Hide Filter | Show/Hide Columns | Show/Hide Snapshot | Export to CSV | Refresh Page

Action	Date Created	File Name	Drift	Risk	Threat	Trust	Computer
<input type="checkbox"/>	Dec 07 2011 08:13:06AM	setup.exe	1	0.0	✓	10	MYCORP\LAPTOP-3
<input type="checkbox"/>	Dec 07 2011 08:14:44AM	test.bat	1	1.3			MYCORP\LAPTOP-3
<input type="checkbox"/>	Dec 07 2011 08:31:30AM	pslist.exe	1	0.0	✓	10	MYCORP\LAPTOP-3
<input type="checkbox"/>	Dec 07 2011 08:25:39AM	autologon.exe	1	0.0	✓	10	MYCORP\LAPTOP-3
<input type="checkbox"/>	Dec 07 2011 08:25:14AM	bginfo.exe	1	0.0	✓	10	MYCORP\LAPTOP-3

### To return to the top-level files view from an associated files report:

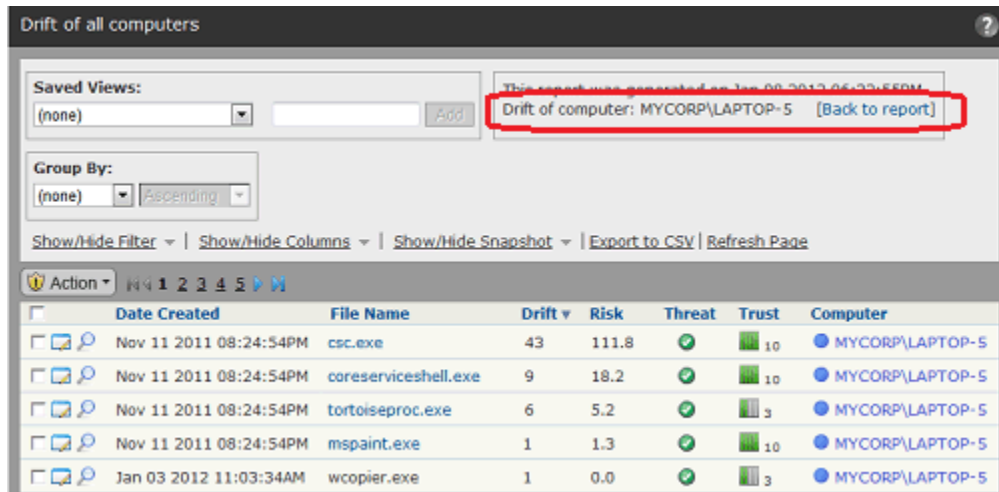
- In the *Files associated with* line above the table, click **[Back to report]**.

## Drift by Files on a Single Computer

You can get a report of drift by files on a single computer. This can be useful in a number of situations; for example, it can help you locate a computer that has significantly more drift than others so that you can take remediation steps.

### To display the drift by files for a single computer:

1. On the console menu, choose **Reports > Baseline Drift**.
2. On the Baseline Drift page, click the name of the report you want to see in the Manage Baseline Drift Reports table.
3. If the Computer View mode is not displayed, click the **Computers** button in the View Mode box.
4. Click the View Details button next to the name of the computer for which you want to see a files report. A report showing only the drifted files on that computer appears.



To return to the top-level Computer view from computer drift details view:

- In the *Drift of computer* line above the table, click **[Back to report]**.

## Responding to Drift Report Results

You can use the results of a Baseline Drift Report for a wide variety of purposes, ranging from simply noting the level of drift to changing the security policy for some or all of your computers. Most of the actions you take can be done in the Bit9 Console, although some of them must be done manually, most notably, restoring missing files. In general, you check the checkbox next to files you want to act on. Many of the choices for responding are on the Action menu.

You can remediate drift in following ways:

- **Add Files to Snapshot:** If the baseline drift report was based on one or more snapshots, you can click the **Show/Hide Snapshots** link and add all files in the report or selected files only to a snapshot. In this case, the files you add are immediately removed from the report and will not become part of subsequent reports. Note that when a file group is checked, all files in the group are added to the snapshot you choose.
- **Locally Approve Files:** Using the Action menu, you can choose **Approve Locally** for checked files in a drift report. In addition to allowing the file to execute on the computer it was found on, this excludes the file from future drift reports if the report excluded all approved files (the default).
- **Remove Local Approval:** Using the Action menu, you can **Remove Local Approval** on checked locally approved files in a drift report.
- **Globally Approve or Ban Files:** Using the Action menu, you can Globally Approve or Globally Ban checked files in a drift report.
- **Create Custom Approvals or Bans:** Using the Action menu, you can choose Approve by Policy or Ban by Policy to create custom approvals or bans for checked files in a drift report. For approvals, you can approve by policy and/or choose to Mark the checked files as installers. For bans, you can ban by policy and choose to block

files banned or just report that they would have been blocked if the ban had been fully enforced.

- **View and Act on Members of a File Group:** If you want to see the details of a file group, you can click on the file name or the View Details button, which shows a page with files in the group that contribute to drift. Here, you can approve or ban files on an individual basis.
- As on other pages in the Bit9 Console, from a drift report you can drill down to the File Details page for access to many of the actions described above.
- **Approve or Ban Files by Group or Trust Methods:** Rather than approving or banning individual files, you can approve the root package that installs a group of files. You might also want to approve files by Publisher, Updater, or User (via the Software Rules page) if you notice that a large number of files from the same source appear in your drift reports and you are willing to trust that source. While making this kind of change will not affect the current report, it will make sure the files covered by the change do not appear in future generations of the report (or other, similar reports) as long as you are not including approved files in the report.
- **Add or Remove Files:** Outside of the console, you can add or remove files from one or more of your systems based on the information in the drift report, reducing the drift shown in future reports.

## Adding Drift Results to a Snapshot

When you view Baseline Drift Report Results, you might see files in the report that you do not want to track for drift. If the drift report uses one or more snapshots as a baseline, you can add files from the drift report to one of the baseline snapshots. You also can create a new snapshot and then add the new snapshot to the baseline.

This type of remediation essentially means you want to ignore certain drift results *in the future*. Nothing is sent to the agents to remove this drift (i.e. change their file inventory), and existing report results remain the same. However, files you add to the snapshot or to a new snapshot you add to the baseline will not be part of future drift report results.

The screenshot shows the Bit9 console interface for a drift report titled "Drift of all computers". The interface includes several controls: "Saved Views" (set to "(none)"), "View Mode" (set to "Files"), "Group By" (set to "(none)"), and "View Mode" (set to "Files"). A "Show/Hide Snapshot" button is highlighted with a red box. Below it, the "Add Files to Snapshot" dialog box is open, showing "Files to add:" with "Checked files" selected, and "Choose existing snapshot:" set to "(none)". The "Create new snapshot:" field is empty. The table below shows drift results for two files: "tortoiseproc.exe" and "set-up.exe". The "set-up.exe" row is highlighted, and its checkbox in the "Add Files to Snapshot" dialog is checked.

Action	Date Created	File Name	Drift	Risk	Threat	Trust	Computer
<input type="checkbox"/>	Dec 07 2011 08:10:02AM	tortoiseproc.exe	14058	43257.5	✓	3	MYCORP\LAPTOP-3
<input checked="" type="checkbox"/>	Dec 07 2011 08:34:13AM	set-up.exe	6504	20558.2	✓	3	MYCORP\LAPTOP-3



**To add files to a snapshot from a baseline drift report:**

1. In the report, unless you plan to add all of the files to a snapshot, check the checkboxes for any files you want to add.
2. Click the **Show/Hide Snapshot** link to display the *Add Files to Snapshot* panel.
3. In the *Add Files to Snapshot* panel, choose the radio button for **All files** or **Checked files** in the *Files to add* line.
4. Specify the snapshot to which you want to add the files:
  - a. If you want to add the files to an existing snapshot, pick one from the *Choose existing snapshot* menu and click **Add**. Note that this menu includes all available snapshots, not just those used as a baseline for the current report.
  - b. If you want to add the files to a new snapshot, type a name in the *Create new snapshot* box and then click the **Create** button.
5. If the report is more than one page long and you are adding checked files, repeat the procedure for each page containing files you want to add.

**Note**

The procedures above assume you are adding to a snapshot to affect future results when the *current* drift report is run, but there are no restrictions on how you use the snapshot. You may save files to a snapshot for some other purpose.

## Creating and Editing Reports

The Add Baseline Drift Report and Edit Baseline Drift Report pages both use the Baseline Drift Report Details window, with only slight variations. Here, we describe creating a report. The procedure for editing the report is essentially the same, except that you start with an existing report.

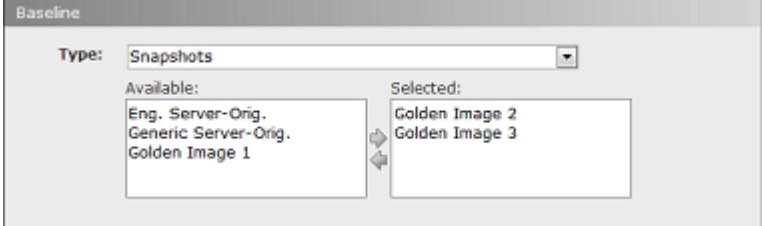
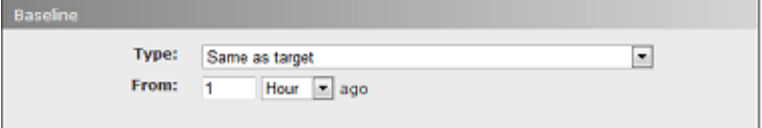


## Creating a Baseline Drift Report

On the Manage Baseline Drift Reports page, clicking on **Add Report** opens the Add Baseline Drift Report page. There, you fill in the details of the report you want to create.

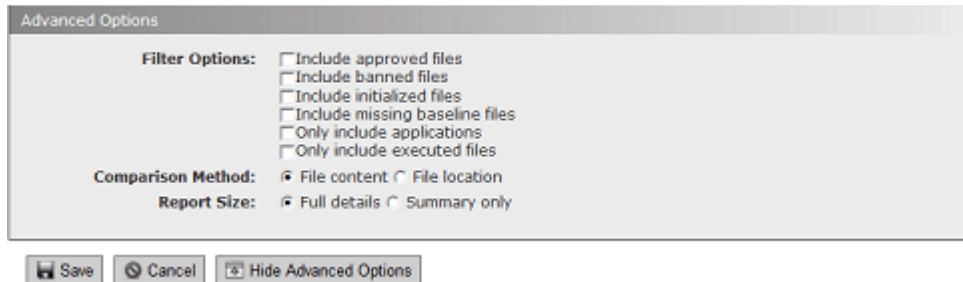
**Table 84:** Add/Edit Baseline Drift Report Details

Item	Description
<b>Copy settings from</b> menu	(Available on the Add page only) Copy settings from an existing report to populate the details of your new report. You can make whatever changes you want to the copy. When you choose a report on this menu, the default name of your new report is <i>Copy of &lt;the name of the existing report&gt;</i> .
<b>Report name</b>	The name that will appear on the Manage Baseline Reports page and the window banner for this report.
<b>Description</b>	Optional text that will help identify the purpose of the report.
<b>Status</b> radio buttons	<b>Enabled</b> means that the report results are automatically generated. <b>Disabled</b> turns off report generation <i>and</i> deletes the entire history of the report.
<b>Target</b> menu	What is to be analyzed in the report. The target Type options are: <b>Computer</b> – Track all file changes on the selected computer. <b>Computers in policy</b> – Track all file changes on all computers in the selected policy. <b>Computer Filter</b> – Track all file changes on computers that match the criteria specified in the filter. <b>Advanced Filter</b> – Track all file changes that match the criteria specified in the filter, which can include both file and computer criteria. <b>All computers</b> – Track all file changes on all computers on your network. For each target Type except <i>All computers</i> , additional fields appear to allow you to complete the specification of the target.

Item	Description
<b>Baseline</b> menu	<p>What the target is compared to. The baseline options are:</p> <p><b>Computer</b> – Compare target to the files found on the named computer at report run time.</p> <p><b>Computers in policy</b> – Compare target to the files found on all computers (at report run time) in the policy selected from this menu.</p> <p><b>Computer Filter</b> – Compare target to files from computers that match the criteria specified in the filter.</p> <p><b>Advanced Filter</b> – Compare target to files that match the criteria specified in the filter, which can include both file and computer criteria.</p> <p><b>Snapshots</b> – Compare target to the files in one or more selected snapshots.</p>  <p><b>Same as target</b> – Compare the files on the target computer(s) to the files on the same computer(s) at a specified point in the past.</p>  <p><b>None</b> – Calculate total drift of all computers without any baseline comparison. This choice generates a report that simply monitors all changes on a target set of machines since the agent was installed. This option does not allow tracking of <i>missing</i> files. If you keep the default Advanced Options, this choice essentially gives you the table of all unapproved files on your target systems, along with additional Drift and Risk information only available in Baseline Drift Reports. You can filter or sort by Risk if you choose to determine whether action is necessary on any of these unapproved files, and also see whether any particular group, user, or computer is contributing disproportionately to total Risk. For each Type choice except <i>None</i>, additional fields appear allowing you to complete specification of the baseline.</p>
<b>Save</b> button	Create the Baseline Drift Report by saving the parameters you have entered. Once created, the report is scheduled to run, unless you disable it.
<b>Cancel</b> button	Cancel the creation or editing of the report.
<b>Show/Hide Advanced Options</b> button	Shows or hides additional parameters for the report. See <a href="#">“Advanced Baseline Drift Report Options”</a> for more details.

## Advanced Baseline Drift Report Options

The Advanced Options section includes options that change the file types considered in a baseline drift analysis, the method of comparison between a baseline and its target, and the level of detail, and therefore the size, of the report when it is generated. Changing these options may affect performance, and also may create reports with considerably more detail for you to examine.



### Advanced Options: File Filter Options

Filter options allow you to choose different types of files to include in the drift report. All of these options are off by default. They are essentially shortcuts for some of the more common options you can set by choosing Advanced Filters in either the baseline or target Type menu. The choices are:

- **Include approved files** – Files with a Local State of *Approved* are included in the baseline drift comparison.
- **Include banned files** – Files with a Local State of *Banned* are included in the baseline drift comparison.
- **Include initialized files** – Files initialized from a newly installed agent are included in the baseline drift comparison.
- **Include missing baseline files** – Baseline drift analysis includes tracking of files that exist in the baseline but are missing on the target systems (does not appear if baseline is Same as Target).
- **Only include applications** – Only files on your network that are executable (e.g., .exe or .com, but not Packages) are included in the baseline drift comparison.
- **Only include executed files** – Only files that actually have executed on your network are included in the baseline drift comparison.

Deciding which of the Filter Options to use depends upon your purpose in running a Baseline Drift Report. Although only unapproved files are included by default, you can run baseline drift reports that include locally Approved and/or Banned files. When both of those options are used, the drift report shows *every* new file of interest, which can be very useful if you want to see whether your systems have “drifted” from a golden image or known baseline. You might discover that some files you have approved should not have been, or that there is a large proliferation of banned files, which, although they cannot execute, indicate a problem.

Another situation in which including locally banned and approved files as well as missing baseline files might be useful is in an environment where systems must be absolutely standard, for example, point-of-sale systems. You can use drift reports to determine whether all your systems *exactly* match your golden disk image.

## Advanced Options: File Comparison Method

Baseline drift reports use both file content (its hash) and file location (its full pathname) to identify added, missing, and changed files. The Advanced Options in Baseline Drift Report Details allow you to change *how* they use these factors:

- **File content** – By default, baseline drift reports use the *File content* method for comparisons. When this option is in effect, if a file in the baseline has the same hash as a file in the target, no drift is reported, regardless of the pathname (location) of the two files. A file in the same location (i.e., same path and filename on baseline and target) but with different hashes is considered modified on the target and so counts as drift. Baseline hashes not found anywhere on the target are reported as *missing files*, and target hashes not found on the baseline are considered *added files*.
- **File location** – If you choose *File location*, no drift is reported for the same hash found with the same path and filename on both baseline and target. Different hashes found at the same location (path and filename) are considered *modified files* and add to the drift number. And if the same hash is found in different locations, it is *not* considered a match. In that case, Baseline Drift Reports may report a new file (if the baseline had no file at the location where the file exists on the target), missing (if the target has no file where the baseline had one), or modified (if there is a file with the same name but a different hash on the baseline and target).

In some cases, the different comparison methods will have no effect on total drift. This is especially likely if you activate tracking of missing files as part of the drift report. If you maintain the default setting, however, and do not track missing files, the different comparison methods can produce different drift results, as the example in [Table 85](#) shows.

**Table 85:** Example: How different comparison methods affect drift

Files in Baseline	Files in Target	Drift by content	Drift by Location
C:\folder1\file1 (hash A)	C:\folder1\file1 (hash A)	None	None
C:\folder1\file2 (hash B)	C:\folder1\file2 (hash F)	1 new (hash F)	1 changed (file2)
C:\folder2\file3 (hash C)	C:\folder2\file3 (hash B)	1 changed (file3)	1 missing (hash C)
C:\folder2\file4 (hash D)		1 missing	1 missing
	C:\folder2\file5 (hash G)	1 new	1 new
<b>Total Drift Including Missing Files</b>		<b>4</b>	<b>4</b>
<b>Total Drift Not Including Missing Files (default)</b>		<b>3</b>	<b>2</b>

## Advanced Options: Report Detail Level

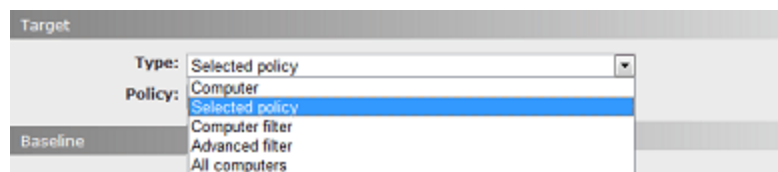
The Advanced Options provide a choice of size for the baseline drift report. The default choice is *Full details*, which generates a drift report that includes details on top-level files and all individual files associated with them. The other choice is *Summary only*, which generates reports that include details at the top level (file group) and shows details on individual files only when requested (i.e., when a user clicks on the file group to get more details). The table shows some of the considerations in choosing one or the other of these options.

**Table 86:** Report Size Options

Differences	Summary Only Report	Full Details Report
Level of Detail	Initially reports results by file groups. Individual-file-level report is generated on demand when you click on a file group.	Contains individual files
Database size	Small size in database	Large size (approx. 10x larger than Summary)
Creation Speed	Faster to generate	Slower to generate
Report Access Speed	Slower to view	Faster to view
Compatibility with Dashboard	Not suitable for graphing (portlets) and extensive analysis because it lacks file-level details such as threat, trust, and publisher/company	Suitable for graphing and analysis by grouping, filtering, etc.

## Using Filters in Target and Baseline Definitions

There are two types of filters on the Type menu for Target and Baseline definitions: Computer Filters and Advanced Filters. Advanced Filters includes all the filters types in Computer Filters. Once you choose the type, you can add as many different filters from its menu as you like. You also can add multiple filters of the same type.



**Computer Filters** are useful if you know that the only criteria you plan to use for specifying a baseline or target are computer-related. You have the following Computer Filter options:

- Computer
- Computer Tag
- IP Address
- Platform
- Policy

Although two of these duplicate choices on the Type menu, by using the Computer Filters type, you allow yourself to set multiple filters for computers. For example, you can specify that you want your baseline to include all computers in Low enforcement policies that have a Computer Tag of “Sales” or “Marketing”.

**Advanced Filters** are useful when you need to include criteria not available on the Computer Filters menu in your specification of a baseline or a target. You can still include computer filters, but Advanced Filters also allow you to use a large set of file criteria, including hash values, file prevalence, and threat level.

While most of the filter choices are self-explanatory, the File Type choice might not be. With the File Type filter, you can specify that your target or baseline includes *or excludes* the following choices:

- **Application:** Any executable (e.g. .exe or .com) except for Packages
- **Supporting File:** Any library loaded by an executable (e.g., .dll, .ocx, .sys)
- **Package:** Any installer (.exe with contents, such as a self-extracting zip or setup program)
- **Script File:** Any script or batch file (e.g., .bat, .vbs, .wsf)
- **Other:** Reserved for future types
- **Unrecognized Executed File:** A file that was not identified as an executable by Bit9 during initialization or later analysis, but that some process attempted to execute. The execution attempt causes the file to be added to the file lists in the Bit9 Console for tracking and management.
- **Unknown:** Files reported by older Bit9 Agents that don't provide file type information

## Drift in Multi-Platform Environments

The Bit9 Security Platform supports installation of agents on Windows, Mac, and Linux computers. Because of the different platform software and applications found on different operating systems, it does not make sense to mix these different computers in a drift measurement. The “noise” level will make extraction of useful data difficult. Targeting all computers or all computers in a policy (unless the policy is platform-specific) in a drift report is not recommended.

If you have a multi-platform environment, possible ways to define a report that produces useful results are:

- Choose **None** as the Baseline Type. This will produce a report that monitors all changes on a target set of machines since the agent was installed, without tracking of missing files. By default, it lists all unapproved files on your target systems, along with additional Drift and Risk information.
- Choose **Same as Target** as the Baseline Type. This will produce a report that shows only the drift of each computer compared to itself.
- For other baseline types, you can create one drift report for each platform by choosing an Advanced Filter or Computer Filter on the Target menu and specifying the platform in that filter.

See [“Creating a Baseline Drift Report”](#) on page 533 for more information about specifying the parameters in a drift report.

## Managing Snapshots

A snapshot is a listing of files (including their name, hash, and location) from one or more computers. You can use a single snapshot or a combination of snapshots as the baseline for a drift report. You can use filters to generate exactly the file list you want and then take a snapshot of that list of files. There are several locations in the Bit9 Console in which you can create snapshots. Once a snapshot is created, you can add or remove files from it as necessary.

Only Power Users, Administrators, and users in custom groups with view and manage snapshot permissions can create, modify and delete snapshots.

**Platform Note:** Mixing files from different operating system platforms (e.g, Windows, Mac, and Linux) in a single snapshot is not recommended.

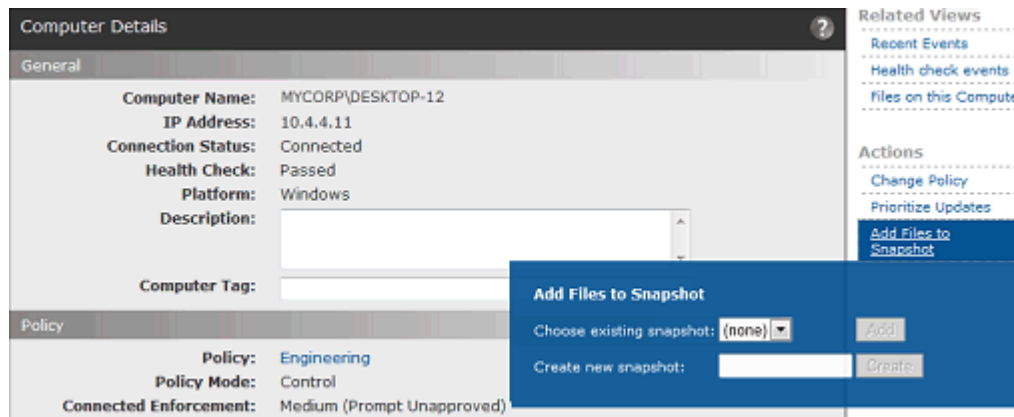
## Creating and Modifying Snapshots

There are two main ways to create a new snapshot:

- using all files on a particular computer
- using a file table, filtered or not, on a console page that includes the Snapshot button

**To create a snapshot (or add to one) from all files on a computer:**

1. On the console menu, choose **Assets > Computers**.
2. In the Computers table, click on the name of the computer whose files you want to use as a snapshot. The Computer Details page appears for that computer.
3. In the Actions menu on the right of the details page, click **Add Files to Snapshot**. The Add Files to Snapshot dialog appears:



4. To *create a new snapshot*, in the dialog, type in the name for the snapshot in the *Create new snapshot* box and click **Create**.

**- or -**

To *add* all of the files on the computer to an existing snapshot, choose an existing snapshot from the *Choose existing snapshot* menu and click **Add**.

A message appears confirming the creation or modification of the snapshot.



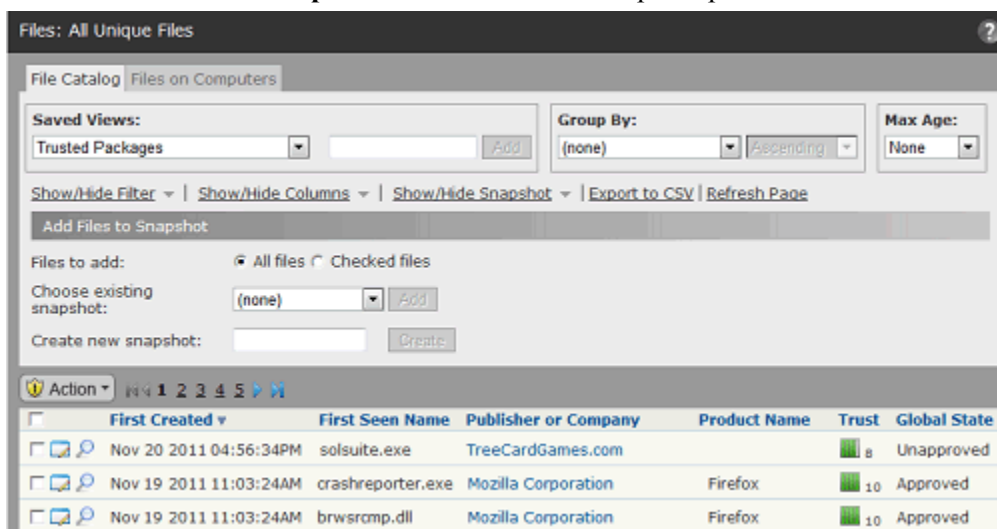
- If you want to view the contents of your snapshot, choose **Reports > Baseline Drift** on the console menu and then click on the **Snapshot** tab.  
Your new or modified snapshot is displayed in the snapshots table.

### Note

A *snapshot* of the files on a computer is static – it is the list of files that were on the computer when the snapshot was taken. You also can use a computer itself as a baseline for comparison, in which case the files on the computer *when you run the report* are the baseline.

### To create a snapshot (or add to one) from a file table:

- Go to the console page from which you want to create the Snapshot.  
For example, choose **Assets > Files** on the console menu to go to the Files page, and then click on **File Catalog**.
- Choose the tabs, filters, columns, and/or Saved View you want to get the list of files you want in the snapshot.
- Click the **Show/Hide Snapshots** link to show the Snapshot panel



- If you want to individually select the files being added to the snapshot, check the box to the left of the file for each file you want to add, and click the **Checked files** radio button in the *Files to add* line of the *Add Files to Snapshot* panel. Otherwise, all files on the page are added to the snapshot.
- To create a new snapshot, in the Snapshot box, type in the name for the snapshot and click **Create**. A new snapshot is created from the current table of files – it includes the files on *all* pages in the table, not just the currently displayed page.  
**- or -**  
To add all of the files in the current table to an *existing* snapshot, choose an existing snapshot from the *Choose existing snapshot* menu and click **Add**.
- If you choose Checked files, you must check and add files for each page in the table – only the files checked on the currently visible page are added.



- If you want to confirm that a new snapshot was created, choose **Reports > Baseline Drift** on the console menu and then click on the **Snapshot** tab. Your new snapshot should be displayed in the snapshots table.


## Viewing and Editing Snapshots

Once created, a snapshot may be viewed on the Snapshot tab of the Baseline Drift page.

**To view a snapshot:**

- On the console menu, choose **Report > Baseline Drift**.
- On the Baseline Drift page, click the **Snapshots** tab.

Name	Date Created	Created By	Number of Files
Golden Image 3	Dec 19 2011 07:43:56AM	rjones@mycorp.local	49757
Golden Image 2	Dec 19 2009 01:03:49PM	admin	14143
Golden Image 1	Nov 24 2009 11:30:19AM	admin	8

- Click either the name of the snapshot you want to view or the View Details button  in its row. The Snapshot Contents page appears, showing a table of all of the files in the snapshot.

File Name	Publisher or Company	Trust	Threat	File State
accountmgr.dll	Microsoft Corporation	10	✓	Unapproved
accountmgr.dll	Microsoft Corporation	10	✓	Unapproved
acctinfo.dll	Microsoft Corporation	10	✓	Unapproved
accwiz.exe	Microsoft Corporation	10	✓	Unapproved
acelpdec.ax	Sipro Lab Telecom Inc.	9	✓	Unapproved
acgenral.dll	Microsoft Corporation	10	✓	Unapproved
aciniupd.exe	Microsoft Corporation	9	✓	Unapproved

From the Snapshot Contents page, you can use any of the standard table tools (filters, column controls, etc.) to change your view of the files in the snapshot.

## Managing Files in Snapshots

You can check one or more files in the snapshot and take the following actions:

- **Remove the checked file(s) from the snapshot** – Files you have checked when you choose **Remove from Snapshot** on the Action menu will be removed from the snapshot, but not from any computers on your network.
- **Approve or Ban the file(s)** – The Action menu provides commands for creating global or custom approvals or bans for checked files in the snapshot. Note, however, that there might be more efficient and flexible approval methods for handling a particular file – for example, approving it by approving its publisher, or by approving the installer that generated the file.
- **Analyze with Bit9 SRS** – Files you have checked when you choose **Analyze** on the Action menu will have information about them supplied by Bit9 SRS.

## Deleting Snapshots

On the Snapshot tab of the Baseline Drift Reports page, you can delete snapshots you no longer need. Before doing so, consider whether the snapshot is really no longer useful, or whether you can make it useful by adding files to or deleting them from it. You cannot recover a deleted snapshot.

**To delete a snapshot:**

1. On the console menu, choose **Reports > Baseline Drift**.
2. On the Baseline Drift page, click the **Snapshots** tab.  
Note that the Snapshots tab does not appear until you have saved at least one snapshot.
3. Click the Delete button in the row of the snapshot you want to delete, and in the confirmation box, click **OK**.

## Displaying Baseline Drift Reports in Graphs

The tables on the Baseline Drift pages provide the greatest detail and flexibility in viewing drift results, but you might want a graphic representation of drift to use as a quick reference indicator of changes in files on your network. You display graphs of Baseline Drift Reports as graphic *portlets* on a *dashboard* page in the console.

The Bit9 Console includes pre-configured portlets, the individual graphs that make up a Dashboard, that provide baseline drift information. You can choose any portlet with “Drift” in its title to see an example of graphic presentation of drift information.

If you plan to create your own drift portlets, consider the following tips for making the information you display usable:

- The horizontal size of portlets varies according to the layout of the dashboard they are displayed on. You may need to move the portlet on the dashboard or change the dashboard layout to accommodate the data in a baseline drift portlet. You also can choose the data and the type of graph you display it in so that the portlet is appropriate for the presentation format.
- Consider how many items will appear on the X axis. The Portlet Editor does allow you to limit the items displayed on the X-axis to the 5, 10, or 15 with the highest or lowest values, but this means you are not seeing all of the data from the report. So if, for

example, you have 1000 computers, you might choose to show drift by *policy* instead of by *computer* – you can always drill down to the more detailed information in console tables. (If you use the “Split by” feature in a portlet, you should similarly limit the number of items that will split the bar, column or other element in your portlet.)

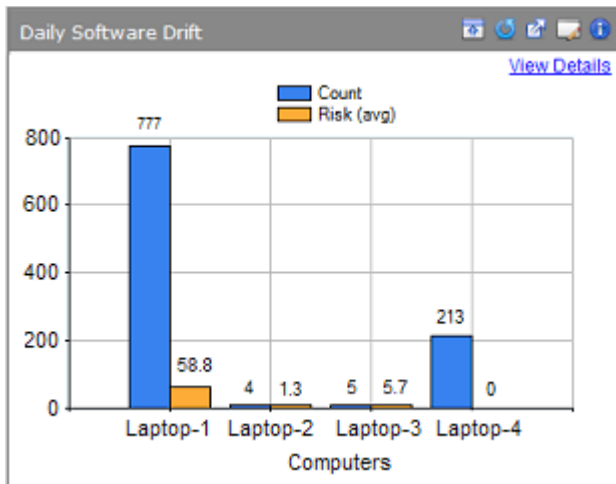
- Use the Preview feature in the Portlet Editor to see how your data will appear. You can try out as many display options as you would like before you Save the portlet.
- If a Baseline Drift Report has a Report Size of *Summary Only* (an option in the Advanced Options when editing or creating a report), it will not have sufficient data for use in the Dashboard. Only reports that have a Report Size of *Full Details* can be displayed graphically.

The example below shows the same information presented in a Baseline Drift Report Results table, and then again in a graphic portlet. On a demonstration system with 5 or fewer Bit9 Agent computers, you will be able to easily view drift by computer in a graph. This is less likely to be useful in a production environment.

In tabular form, the drift report might look something like the following figure.

Computer	Drift	Risk	Policy
MYCORP\LAPTOP-1	777	58.8	IT Group
MYCORP\LAPTOP-4	213	0.0	Engineering1
MYCORP\LAPTOP-3	5	5.7	Engineering2
MYCORP\LAPTOP-2	4	1.3	Testing Group

The same information in a Dashboard would appear as shown in the next figure. Clicking View Details brings you back to the full report table.



For more information about dashboards, see “Using and Customizing Dashboards” on page 567.

## Creating Baseline Drift Alerts

You can create an Alert to notify you and any other console users that baseline drift has crossed a threshold that you have set. When you enable a baseline drift alert, the triggering conditions are evaluated each time the report generation is complete.

### To create a baseline drift alert:

1. On the console menu, choose **Tools > Alerts**. The Alerts page, which lists all configured alerts, appears:
2. From the Alerts page, click the **Add Alert** button. The Alert Information page appears:

The screenshot shows the 'Alert Information' window with the following configuration:

- General:** Alert Name: [empty], Message: [empty], Status:  Enabled  Disabled
- Type:** Type: Baseline Drift Alert (highlighted with a red box), Description: Alerts subscribers when baseline drift factor reaches specified threshold, Mail Template: Default
- Criteria:** Drift Report: Drift of all computers (highlighted with a red box), Alert When: Total risk [dropdown] per computer reaches [dropdown] 1 (highlighted with a red box)
- Subscribers:** Note: Alert must be created before email recipients can be specified
- Reminder Mail:** Status:  Enabled  Disabled, Remind Every: 1 day(s)

Buttons: Save, Cancel

3. In the General panel of the Alert Information window, enter an Alert name and a Message (what will be sent to subscribers when the alert is triggered).
4. In the Type panel, choose **Baseline Drift Alert** from the Type menu.
5. In the Criteria panel, choose the drift report whose data the alert should monitor.  
**Note:** If no drift reports have been created yet, the Drift Report line will display a message to that effect instead of the menu.
6. In the *Alert when* line, choose threshold parameters at which you want an alert to be triggered.
7. Click **Save** to create the alert.
8. On the Alerts page, click the View Details (pencil and file) button next to the name of your new alert.

9. On the Alert Information page, in the Subscribers section, enter each email address to which you want alert email sent and click **Add** after each one.
10. If you want to specify the email format, choose one from the menu to the right of the address box.
11. If you want to resend alert emails periodically as long as the alert is not reset, set Reminder Mail to **Enabled** and choose a time interval.
12. .Click **Save**.

Each time baseline drift conditions exist that meet the triggering conditions, the console highlights that alert in color and adds a Reset button, both on the Home page dashboard and the Alerts page. It also sends email about the condition to all subscribers to this alert. You can reset the alert manually by clicking the Reset button next to its name on the Alerts page. Baseline Drift alerts automatically reset when the drift in the specified drift report falls below the specified threshold for the specified parameter (user, computer, or policy).

See [“Using Bit9 Alerts”](#) on page 494 for more on alert behavior.



## Chapter 20

# Advanced Threat Detection

This chapter describes how you enable and use Bit9's Advanced Threat Indicators, and how you can monitor threats through Bit9 events, file details, and alerts.

**Sections**

Topic	Page
<a href="#">Overview</a>	548
<a href="#">Indicator Sets for Threat Detection</a>	549
<a href="#">Indicator Set Exceptions</a>	553
<a href="#">Monitoring Threat Reports</a>	558
<a href="#">Threat Views on the Events Page</a>	558
<a href="#">Threat Events in Syslog Output</a>	561
<a href="#">Threat Views on the Files Pages</a>	562
<a href="#">Threat-Related Alerts</a>	562
<a href="#">Responding to Threats</a>	563

## Overview

The Bit9 Security Platform includes many features that help you monitor activities on your endpoints. To enhance these capabilities, Bit9 provides a set of advanced detection features, including:

- **Advanced Threat Indicators (ATIs)**, which are rules grouped in Indicator Sets that aid in detecting particularly threatening or suspicious activity on systems reporting to your Bit9 server
- **Detection Views** into your Bit9 database that highlight detection-related data provided by the ATIs and other Bit9 Security Platform features

Advanced Threat Indicators may indicate malicious activity based on an event or sequence of conditions on an endpoint. This has the potential to provide broader coverage and earlier warning than a detection system relying solely on a snapshot of a point in time, such as an Indicator of Compromise (IOC) that only reports on the existence of a file or registry setting after the fact. Because advanced detection also uses dynamic events as part of its implementation, it can provide real-time indication of suspicious activity and capture metadata for related events, such as the creation of a suspicious file.

While ATIs are strictly for reporting purposes, you may be able to remediate a detected threat using other Bit9 capabilities, or by actions outside of the Bit9 Console. For example, you could create a ban for a file reported as a threat or create a custom rule that bans an action in a particular location when conducted by a certain process. Also the Bit9 Event Rule capability allows you to immediately ban *any* file that appears in a threat-related event.

The summary steps for using Advanced Threat Detection are:

- **Enable Indicator Sets for Detection** – On the console Indicator Sets page (**Rules > Indicator Sets**), enable the Indicators Sets that you want activated. Once the Indicator Sets are enabled on the server, the ATIs are committed to all the agents and will result in new events being sent to the server when the conditions specified by any of the ATIs occurs. See [“Indicator Sets for Threat Detection”](#) on page 549.
- **Monitor Threat Reports** – Periodically check for suspicious or threatening events or files using the Saved Views on the Events and Files pages. See [“Monitoring Threat Reports”](#) on page 558.
- **Fine-tune Reporting** – If you see detection related events that you do not want reported, either disable the Indicator Set that detected them (if you are sure you do not want any reports from that Indicator Set) or create an Indicator Exception for the specific file reported in the event. See [“Indicator Set Exceptions”](#) on page 553. On the other hand, if you see detection-related events that you consider high priority, consider creating alerts for those events. See [“Threat-Related Alerts”](#) on page 562.
- **Remediate Threats** – If you see a threat that must be remediated, consider creating a Bit9 rule (for example, a ban, custom rule, or event rule) to prevent malicious action by the threat and/or take action outside of Bit9 (for example, deleting files or creating firewall rules) to respond to the threat. See [“Responding to Threats”](#) on page 563.

ATIs work with agents at any Enforcement Level (other than Disabled), although the conditions that lead to threat detection should be less likely in High Enforcement.



### Upgrade Note

If you used the separately installed Advanced Detection features in Bit9 7.0.0 or 7.0.1, be aware that in the Bit9 Security Platform v7.2.1, ATIs are grouped in Indicator Sets rather than Updaters. This means that you view, enable, and disable Indicators on the Indicator Sets page. Also, if you created an ATI-related Event Rule in one of these prior 7.0.x releases, you must create a new Event Rule that reflects the 7.2.1 implementation. There is, however, a Saved View on the Events page – *Threat Reports - Legacy* – that will show you threats reported by the previous ATIs.

See the *Bit9 Security Platform Release Notes* for this release for a complete description of the steps needed to convert to the new version of detection, and for steps to make sure you have the latest available ATIs.

## Indicator Sets for Threat Detection

An Indicator Set is a group of ATIs (detection rules) in the category and for the platform specified by its name. Viewing and managing Indicator Sets requires that the console user has *Manage indicator sets* permission enabled. This permission is enabled by default for Administrators and Power Users. See “[Account Group Permissions](#)” on page 93 for details on enabling user permissions

The following list describes default Indicator Sets provided with the initial release of v7.2.0 and the types of ATIs they contain. Note that Indicator sets may be added, removed, or modified in cloud-based updates or future versions of the Bit9 Security Platform. See “[Updates to Indicator Sets](#)” on page 557 for more details.

- **Windows Application Behavior** – The ATIs in this group detect behavior that is not normally expected from the type of application performing it. For example, one ATI in this group, called “Possible exploit of document handling application”, reports an event if an application such as Microsoft Excel creates an unknown executable (e.g., foo.exe).
- **Windows Process Injection** – The ATIs in this group detect injection of suspicious code into specific system processes. For example, one ATI in this group, “Possible password hash tool execution”, reports an event if a process tries to harvest cached password hashes on a system. In general, this indicator set reports issues involving memory rules.
- **Windows Startup Configuration** – The ATIs in this group detect suspicious changes to the Windows startup configuration.
- **Windows Suspicious Based on File Name** – The ATIs in this group detect files whose names indicate that they are suspicious or malicious. For example, if a file has a name or file extension that is similar to a legitimate file (e.g., “iexplore.exe”) but is modified slightly (e.g., “Lexplore.exe”), a ATI in this group reports it. Files with the names of known malware or suspicious extensions are also reported.
- **Windows Suspicious Based on Path** – The ATIs in this group detect file activity in suspicious location, such as file execution in the Recycle Bin or System Volume.
- **Windows Suspicious Based on Path and File Name** – The ATIs in this group detect suspicious activity based on both file path and file name. For example, one ATI

- reports System files executing outside system folder. Another indicator in this group reports execution of rarely used system utilities.
- **Windows System Configuration** – The ATIs in this group detect suspicious system configuration activity, such as firewall or name resolution tampering, or installation of a language pack.
  - **Mac Application Behavior** – The ATIs in this group detect behavior that is not normally expected from the type of application performing it. For example, one ATI in this group reports an event if an application such as Microsoft Excel creates an unknown executable. Another ATI in this group detects shells being spawned from a browser.
  - **Mac Shell Activity** – The ATIs in this group detect suspicious use of a command shell.
  - **Mac Suspicious Based on Path** – The ATIs in this group detect activities that are suspicious because of where they are attempted, such as execution attempts from the Trash folder.
  - **Mac System Configuration** – The ATIs in this group detect suspicious changes to system configuration, such as attempts to escalate privileges.
  - **Linux Possible Backdoor** – The ATIs in this group detect files associated with backdoors to the Linux secure shell.
  - **Linux Startup Configuration** – The ATIs in this group detect suspicious changes to the Linux startup configuration.
  - **Linux System Configuration** – The ATIs in this group detect suspicious changes to the Linux startup configuration, such as name resolution tampering.

**To view, enable or disable Indicator Sets:**

1. On the console menu, choose **Rules > Indicator Sets**. The Indicator Sets page appears.

<input type="checkbox"/>	Indicator Set Name ▲	Version	Enabled	Platform	Policy	Date Updated
<input type="checkbox"/>	Linux Possible Backdoor	1	No	Linux	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Linux Startup Configuration	1	No	Linux	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Linux System Configuration	1	No	Linux	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Mac Application Behavior	1	No	Mac	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Mac Shell Activity	1	No	Mac	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Mac Suspicious Based on Path	1	No	Mac	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Mac System Configuration	1	No	Mac	All Policies	Apr 25 2014 02:38:45 PM
<input type="checkbox"/>	Windows Application Behavior	1	No	Windows	All Policies	Apr 25 2014 02:38:42 PM
<input type="checkbox"/>	Windows Process Injection	1	No	Windows	All Policies	Apr 25 2014 02:38:43 PM
<input type="checkbox"/>	Windows Startup Configuration	1	No	Windows	All Policies	Apr 25 2014 02:38:44 PM
<input type="checkbox"/>	Windows Suspicious Based on File Name	1	No	Windows	All Policies	Apr 25 2014 02:38:44 PM
<input type="checkbox"/>	Windows Suspicious Based on Path	1	No	Windows	All Policies	Apr 25 2014 02:38:44 PM
<input type="checkbox"/>	Windows Suspicious Based on Path and File Name	1	No	Windows	All Policies	Apr 25 2014 02:38:44 PM
<input type="checkbox"/>	Windows System Configuration	1	No	Windows	All Policies	Apr 25 2014 02:38:44 PM

2. Check the box next to the name of each indicator set you want to enable and then choose **Enable Indicator Sets**.  
- *or* -  
Check the box next to the name of each indicator set you want to disable and then choose **Disable Indicator Sets**.
3. To see details and exceptions for any one Indicator Set, click the View Details button next to its name in the table.

Initially, all Indicator Sets are disabled. You can enable and disable these rule groups as you choose. For example, if one Indicator Set is generating too many events not of interest in your environment, you can turn it off on the Indicator Sets page. You also can create exceptions to an Indicator Set without disabling all of the indicators in the set. See [“Indicator Set Exceptions”](#) on page 553 for more details.

As with other Bit9 tables, you can use the Group By menu, the Show/Hide Filter link and the Show/Hide Columns link to modify your view of the Indicator Sets table. [Table 87, “Indicator Set Parameters”](#) on page 552 provides a description of all available columns.

## Indicator Set Details

In the Indicator Sets table, clicking on the View Details button next to the name of a set opens the Indicator Set Details page for that set. This page includes:

- key details about the Indicator Set, including its name, version, and history

- radio buttons and checkboxes for enabling and disabling the Indicator Set, and for specifying the policies in which the set is active
- an Exceptions panel that shows any exceptions to the Indicator Set and allows them to be enabled, disabled, and deleted
- a Recent Events link in the Related Views menu that opens the Events page filtered to show recent events involving this Indicator Set

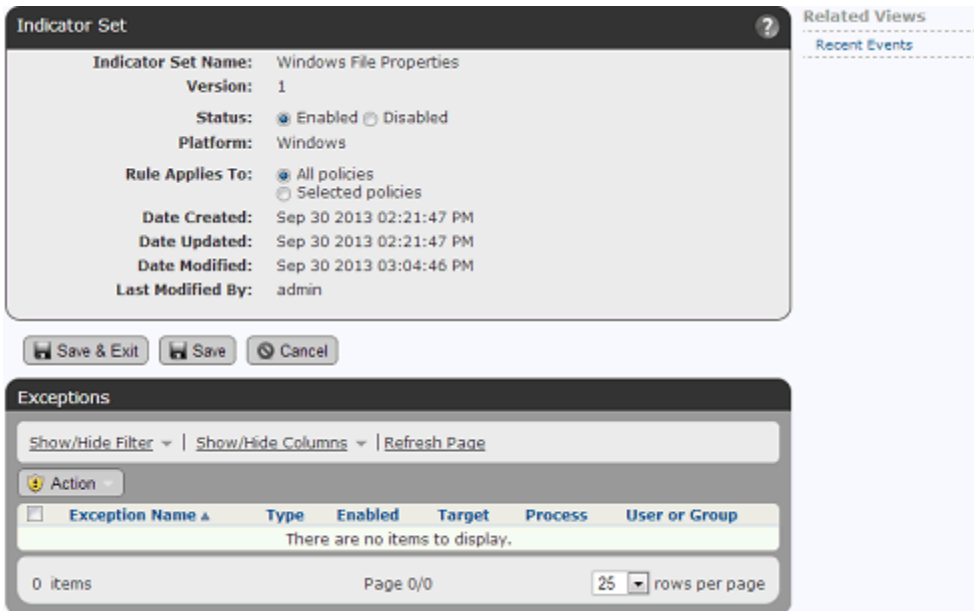


Table 87 shows the fields available in the Indicator Sets table and the Indicator Set Details page.

**Table 87:** Indicator Set Parameters

Field	Description
<b>Indicator Set Name</b>	Name of the Indicator Set. Names are assigned by Bit9 and describe and include the platform and general purpose of the ATIs in the set.
<b>Version</b>	The version of this Indicator Set. If new versions have been downloaded from the Bit9 cloud, the version number will increment to indicate this.
<b>Status</b> (Details page) <b>Enabled</b> (Table)	On the Details page, Status radio buttons make this Indicator Set Enabled or Disabled. In the Indicator Sets table, the Enabled field shows 'Yes' or 'No'.
<b>Platform</b>	Platform (Windows, Mac, or Linux) for which this Indicator Set is effective.

Field	Description
<b>Rule Applies To</b> (Details page) <b>Policy</b> (Table)	On the Details page, the radio buttons allow you to apply the rule to <b>All policies</b> or <b>Selected policies</b> . If you choose <b>Selected policies</b> , a list of all policies on your Bit9 Server appears, each with a checkbox.  In the Indicator Sets table, the Policy field shows which policies the set is activated for.
<b>Date Created</b>	Date and time this Indicator Set was first seen on this Bit9 Server.
<b>Date Updated</b>	Date and time this Indicator Set was last updated to a new version. If there have been no updates to this Indicator Set, this is the same as Date Created.
<b>Date Modified</b>	Date and time of the last <i>user-initiated</i> change to the Indicator Set configuration. This includes enabling or disabling the Indicator Set and changes to the policies it applies to.
<b>Last Modified By</b>	Bit9 Console user that made the most recent change to editable parameters of this Indicator Set
<b>Exceptions Panel</b> (Details page only)	On the Details page, this panel lists any exceptions made for this Indicator Set. See <a href="#">“Indicator Set Exceptions”</a> on page 553 for more on exceptions and <a href="#">Table 88, “Exception Details (in Indicator Sets)”</a> on page 556 for a description of Indicator Set Exception parameters.

## Indicator Set Exceptions

Indicator Set Exceptions are modifications of the Indicator Set that eliminate reports for actions that match the exception. They allow you to reduce or eliminate reporting of events that are not of interest to you while still leaving the rest of the Indicator Set functionality enabled. To create an Indicator Set exception, you identify an ATI-related event on the Events page that you would like to remove from future reporting. You can create an exception specific to that event automatically, or you can modify the exception so that applies to a broader or narrow range of targets, processes, or users.

Indicator Set Exceptions are specific to the Indicator Set that generated the event you use to create them. You can create multiple exceptions at once, but you cannot create an exception using a non-ATI-based event.

### To create Indicator Set Exceptions (default method):

1. If the events for which you want to create exceptions are not displayed, on the console menu, choose **Reports > Events** and choose the **Threat Indicators** Saved View. You can also choose an event from another view, but using Threat Indicators ensures that the events shown all have an associated Indicator Set.  
**Note:** You also can choose the **Recent Events** link on an Indicator Set Details page to see all recent events for that set.
2. If necessary, change the Max Age value to view older events.

3. When one or more events for which you want to create an exception are displayed, check the box next to each one and on the Action menu, choose **Create Indicator Set Exceptions**. A status message at the top of the page will indicate if the exceptions have been successfully created, or will show an error if they have not. A common error is selection of an event that does not have an Indicator Set.

Each exception created in this way uses the name of the Indicator Set plus incrementing digits (e.g., the first exception to the Windows System Configuration set is named “Windows System Configuration Exception 1”).

You can edit an Indicator Set Exception once it is created (including its name), or you specify special parameters at the time of creation by choosing an *Create an advanced Indicator Set Exception*. Note that an advanced Indicator Set Exception may be created for only one event at a time.

**To create an advanced Indicator Set Exception:**

1. If the event for which you want to create the exception is not displayed, on the console menu, choose **Reports > Events** and choose the **Threat Indicators** Saved View. You can also choose an event from another view, but using Threat Indicators ensures that the events shown all have an associated Indicator Set.  
**Note:** You also can choose the **Recent Events** link on an Indicator Set Details page to see all recent events for that set.
2. If necessary, change the Max Age value to view older events.
3. When the event for which you want to create an advanced exception is displayed, check the box next to it and on the Action menu, choose **Create an advanced Indicator Set Exception**. The Add Indicator Set Exception dialog appears with the Indicator Set and Platform entered in read-only form and the other parameters editable. Note that if you check more than one box, an error message appears.
4. In the Add Indicator Set Exception dialog box, enter an Exception Name and optionally a Description.
5. Edit the other parameters to create the rule you want. These parameters are described in [Table 88, “Exception Details \(in Indicator Sets\)”](#) on page 556.
6. When you have finished configuring the exception, click the **Save** button if you want to stay on the page or the **Save & Exit** button to return to the Events page.

The new exception appears in the Exceptions panel of the Indicator Set Details page.

## Indicator Set Exception Details

Each Indicator Set Details page includes an Exceptions panel. If exceptions have been created for this set, they appear in a table in that panel.

**Indicator Set Details**

Indicator Set Name: Windows System Configuration  
 Version: 1  
 Status:  Enabled  Disabled  
 Platform: Windows  
 Rule Applies To:  All policies  Selected policies  
 Date Created: Feb 12 2014 11:52:10 AM  
 Date Updated: Feb 12 2014 11:52:10 AM  
 Date Modified: Feb 19 2014 02:52:20 PM  
 Last Modified By: admin

Save & Exit Save Cancel

**Exceptions**

Show/Hide Filter | Show/Hide Columns | Refresh Page

Action

Exception Name	Type	Enabled	Target
Windows System Configuration Exception 1	Path	Yes	c:\windows\system32\drivers\etc\hosts
Windows System Configuration Exception 2	Registry	Yes	\registry\machine\system\controlset001\ser

The table shows the Exception name and other details of the exception, and like other Bit9 tables, it can be modified using the Show/Hide Filter and Show/Hide Columns links. The Action menu allows you to Enable, Disable, and Delete exceptions.

When you click on the View Details button for an exception in the table, the Indicator Set Exception Details page appears.

**Edit Indicator Set Exception**

General

Indicator Set Name: Windows System Configuration  
 Indicator Name: Windows firewall tampering  
 Exception Name: Windows System Configuration Exception 2  
 Description:  
 Status:  Enabled  Disabled  
 Platform: Windows

Definition

Type: Registry  
 Target: Specific Path...  
 \registry\machine\system\controlset001\services\shared;  
 Process: Specific Process...  
 c:\windows\system32\reg.exe  
 User Or Group: Local System

Save & Exit Save Cancel

**Table 88:** Exception Details (in Indicator Sets)

Field	Description
<b>Indicator Set Name</b>	Name of the Indicator Set to which this exception is applied. Names are assigned by Bit9 and describe and include the platform and general purpose of the ATIs in the set.
<b>Indicator Name</b>	Name of the specific ATI in the Indicator Set for which an exception is being made
<b>Exception Name</b>	Name of this exception. This is provided automatically if the exception is created using the <b>Create Indicator Set Exceptions</b> command on the Action menu. Automatic naming uses the name of the Indicator Set plus incrementing digits (e.g the first exception to the Windows System Configuration set is named "Windows System Configuration Exception 1". If the Exception is created using <b>Create an advanced Indicator Set Exception</b> , the name is entered by the console user. In either case, the name may be changed later.
<b>Description</b>	Additional information about the exception. This can be any text you choose to enter. (Optional)
<b>Status</b>	Radio buttons that Enable or Disable this exception.
<b>Platform</b>	Platform (Windows, Mac, or Linux) to which this Exception applies.
<b>Type</b>	The type assigned to this exception when it was created (not editable). The possible values are Path, Process and Registry.
<b>Target</b>	<p>The Target of the action for which the exception was created. There may be multiple values in this field, and the values that are used depend upon the Exception Type:</p> <ul style="list-style-type: none"> <li>• Path – File paths or file names</li> <li>• Process – Processes</li> <li>• Registry – Registry paths</li> </ul> <p>Specification of paths and processes in Bit9 rules is described in the Custom Rules chapter: "<a href="#">Specifying Paths and Processes</a>" on page 345 shows details on specifying a process in Bit9 rule pages and <a href="#">Table 51</a> shows process menu options.</p>
<b>Process</b>	This menu allows you to limit the exception so that it is applied only when certain processes attempt to take action matching the target specification. " <a href="#">Specifying Paths and Processes</a> " on page 345 shows details on specifying a process in Bit9 rule pages.
<b>User or Group</b>	The users or groups to which this exception applies. Specification of users and groups is described in the Custom Rules chapter, in the section " <a href="#">Specifying Users or Groups</a> " on page 353.
<b>Date Created</b> (Table only)	Date and time this Exception was created.



Field	Description
<b>Date Modified</b> (Table only)	Date and time this Exception was last modified.
<b>Created By</b> (Table only)	Bit9 Console user that created this Exception
<b>Last Modified By</b> (Table only)	Bit9 Console user that last modified this Exception

## Updates to Indicator Sets

Bit9 provides a mechanism for automatic periodic updates to Indicator Sets. This may involve entirely new Indicator Sets, new indicators added to existing sets, reorganization of Indicators Sets, or changes to existing indicators. These changes are delivered automatically when available if you have Bit9 SRS enabled and have also enabled automatic Indicator Set updates on the System Confirmation/Advanced Options page. See [“Activating Bit9 SRS”](#) on page 643 for more information about enabling Bit9 SRS and [“Advanced Configuration Options”](#) on page 627 for more information about enabling automatic Indicator Set updates.

You may leave automatic updates enabled or temporarily enable updates periodically if you choose. Updates are scheduled to be delivered within 24 hours and often appear sooner than that.

If you receive automatic updates, the state of Indicator Sets is as follows:

- New Indicator Sets are added in a disabled state.
- Existing Indicator Sets remain enabled or disabled according to the state they were in prior to updating. This is true even if the upgrade adds or modifies threat indicators in the existing Indicator Set.

## Tracking Indicator Set Updates

There is a built-in **Indicator Set Alert** that, when enabled, will inform you of the following Indicator Set changes:

- Indicator Set updated
- Indicator Set created
- Indicator Set deleted

This alert may be especially useful if you are only enabling the automatic updates temporarily – you will know when to turn off the updates. See [“Using Bit9 Alerts”](#) on page 494 for more on enabling and configuring alerts.

You can also tell whether a detection Indicator Set has been updated by reviewing Version, Date Created, and Date Updated fields on the Indicator Set Details page or Indicator Sets table.

## Monitoring Threat Reports

Suspicious or threatening activity is reported through Saved Views on the Bit9 Console Events page and the Files pages. You should periodically check these views as part of your threat monitoring activity. In addition to providing information, monitoring these threat reports also helps you take actions to improve reporting and remediate threats:

- **Create Indicator Set Exceptions** – If you see specific threat-related events that you do not want reported, you can create Indicator Set Exceptions to eliminate reporting of those events. See [“Indicator Set Exceptions”](#) on page 553.
- **Disable Indicator Sets** – If you determine that a particular Indicator Set always reports events that are not of interest to you, you can disable the Indicator Set. See [“Indicator Sets for Threat Detection”](#) on page 549.
- **Enable Indicator Sets** – If you have not enabled all Indicator Sets and you think that certain critical activity is not being reported, see whether the disabled Indicator Sets would report that activity. See [“Indicator Sets for Threat Detection”](#) on page 549.
- **Create Alerts** – If you see detection-related events that you consider high priority, consider creating alerts for those events. See [“Threat-Related Alerts”](#) on page 562
- **Remediate Threats** – As you monitor threats, you may see events that require remediation. This remediation might involve actions done outside of Bit9, creation of Bit9 rules, or some combination of the two. See [“Responding to Threats”](#) on page 563.

## Threat Views on the Events Page

On the Bit9 Console Events page, suspicious or threatening activity is reported in several Saved Views, some of which require Indicator Set activation and some of which use other data. The following Saved Views are threat-related:

- **Threat Indicators** – This view shows threats detected by the ATIs in the Indicator Sets on Bit9-managed computers. If no Indicator Sets have been activated, this view will be empty. More details about these reports are shown below in the section [“Reviewing Threat Event Reports”](#) on page 559.
- **Threat Indicators - Legacy** – This view shows threats detected by the ATIs that were installed in releases prior to v7.2.0. If you did not install the Detection Enhancement in a prior release, this view will be empty.
- **Threat Report - Suspicious executable created by shell** – This view shows events in which certain executable files are created by cmd.exe or powershell.exe in locations such as the system directory, RecycleBin, or AppData.
- **Threat Report – Suspicious Files by Location** – This view shows events in which a file is first seen or executed on any computer, or first appears (unapproved) on at least one computer, in an unusual, suspicious location. An example would be unexpected file activity in the Recycle Bin.
- **Threat Report – Suspicious Files by Name** – This view shows events in which a file is first seen or executed on any computer, or first appears (unapproved) on at least one computer, with a suspicious name, often a name that appears similar to the name of a legitimate Windows file. For example, discovery of a file named svch0st.exe (using a zero in place of the lowercase ‘o’ in svchost.exe) would appear in this event view.
- **Threat Report – Suspicious Files by Parent** – This view shows events in which an unknown, or low prevalence, executable file is written by a program that should not

normally be creating such files. An example of this would be an executable file created by Adobe Reader; this is often indicative of a malformed- or malicious-PDF-style attack.

#### To view threat reports on the Events page:

1. Choose **Reports > Events** on the console menu.
2. On the Saved Views menu, choose the **Threat** view you want to examine.

### Fields in Threat-Related Events Views

Certain fields in the Events table are of particular interest in the Threat views. Some are visible in the table by default and some may be added. They include:

- **Indicator Set** – The name of the Indicator Set containing the indicator that triggered the event.
- **Rule Name** – The name of the rule that triggered the event. For detection events, these are descriptions of the suspicious activity being detected.
- **Indicator Name** – This optional field is the same as the Rule Name for threat events. It is included to make it easier to identify threat events in Syslog output.
- **Process Threat** – The threat level for the process attempting an action in this event, if reported by the Bit9 Software Reputation Service (SRS).
- **Process Trust** – The trust level for the process attempting an action in this event, if reported by Bit9 SRS.
- **Process Prevalence** – The prevalence of the file associated with the Process field of the event. Prevalence is the number of computers on which at least one instance of the process file exists.
- **File Threat** – The threat level for the file acted upon in this event, if reported by Bit9 SRS.
- **File Trust** – The trust level for the file acted upon in this event, if reported by Bit9 SRS.
- **File Prevalence** – The prevalence of the file acted upon (the file in the File Name field) in this event. Prevalence is the number of computers on which at least one instance of the file exists.

#### Note

The initial values and later updates to threat, trust and prevalence data are provided based on access to Bit9 SRS and scheduling of Bit9 tasks, and updates may have a delay.

### Reviewing Threat Event Reports

Different event views provide different types of information, and cover different time windows.

The **Threat Indicator** view is likely to show the most recent or serious potential threats. Because of this, you might choose to concentrate on this view first. However, keep in mind that the Threat Indicators view shows only matching events that occur *after* you enable one or more Indicator Sets.

For an event in the Threat Indicators view, both the Indicator Set and the Rule Name are shown for the ATI that triggered the event. This shows you the type of threat the rule identified. It also provides a way to identify the source of over-reporting or false positives, and so helps you decide whether you want to disable an Indicator Set or create an exception for certain rules within it.

The **Threat Report** views make use of standard Bit9 events, including those that were present before you added the enhancement. They can report on matching events for whatever time period you choose on the Max Age menu, regardless of whether you have any of the Indicator Sets enabled. Like all events views, the maximum time frame for which threat events can be viewed is delimited by the database trimming choices in effect for your Bit9 database.

The Description field is also useful when you are reviewing events. Depending upon the event, it may identify the file that was written, modified or deleted, the process that acted on the file, and other pertinent data. For example, events generated by the following ATIs might have these descriptions:

Rule Name	Sample Description
Suspicious executable based on name	File 'c:\documents and settings\user\temp\explore.exe' was modified or deleted.
Unusual change to startup configuration	Modification of registry 'registry\machine\software\microsoft\windows nt\currentversion\winlogon\shell' was allowed.

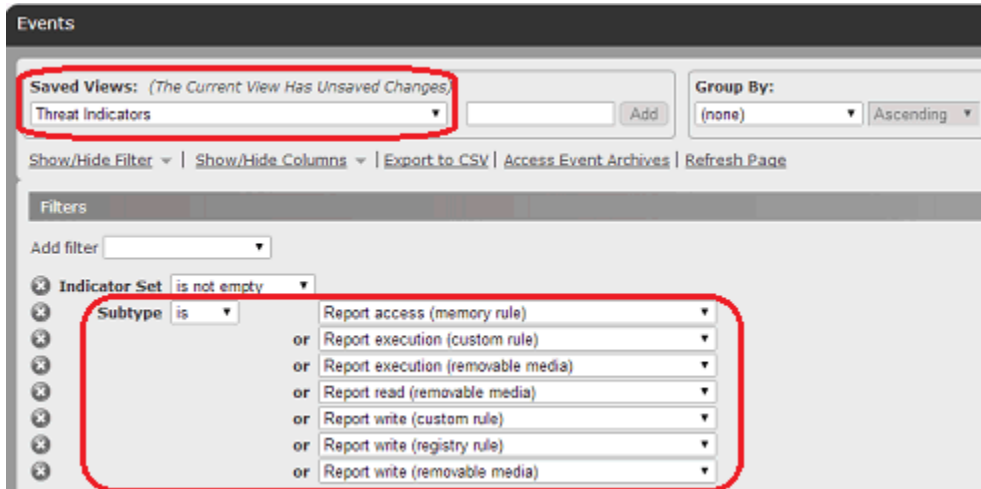
Some of the information in the description is also available in specific fields that you can add to the view.

**Note**

Unlike the event views, the File Catalog view reports on both existing and historical files in the file inventory. If a file matching the view parameters ever existed on an agent-managed computer reporting to your server, it will be included in the view.

## Showing and Modifying View Parameters

You can view the filters that are used to create the threat-related event views by clicking on the Show/Hide Filter button when the view is being displayed. The example below shows the filters used to build the Threat Indicators view.



You can modify these views to add, remove, or modify filter conditions to further refine the view to either eliminate un-interesting events or broaden the scope of events displayed. Although modifications of default Saved Views cannot be saved, you can save your modified view under a new name.

By default, events from the past day are shown in the threat views. You can choose a different time period on the Max Age menu on the Events page.

## Threat Events in Syslog Output

Threat-related events are exported to Syslog with other Bit9 events. To decide what to filter or search for in Syslog, you can choose one of the Threat views and review the Rule Names shown in the table to see the specific rules that generated an event. You also can search for any event in Syslog that contains an Indicator Name field (“indicatorName” in raw output, mapped to different strings depending upon format), which will identify it as a threat detection event. For these events, Indicator Name is the same as Rule Name.

Timestamp	Indicator Set	Rule Name
Feb 19 2014 03:29:03 PM	Windows Suspicious Based on File Name	Suspicious executable based on extension
Feb 19 2014 03:28:59 PM	Windows Suspicious Based on Path and File Name	Suspicious executable based on location
Feb 19 2014 03:28:48 PM	Windows Startup Configuration	Unusual change to startup configuration
Feb 19 2014 03:28:48 PM	Windows Startup Configuration	Unusual change to startup configuration
Feb 19 2014 03:28:41 PM	Windows System Configuration	Possible name resolution tampering
Feb 19 2014 03:28:34 PM	Windows Suspicious Based on Path	File execution from Recycle Bin

One other potential search approach is to filter Syslog output to show just event subtypes that begin with "Report " (except for "Report execution block") – these are the subtypes for threat-related events. To see the specific list of event subtypes for an Events page view, you can choose the view from the Saved Views menu and then click on **Show/Hide Filter**.

See the separate document *Bit9 Events Integration Guide* for more information on the Syslog output available from the Bit9 Server.

## Exporting Threat Event Data to CSV Files

As with other tables in the Bit9 Conole, data in threat-related tables on the Events page may be exported to CSV files, which can be useful for analysis of threats in external tools. If you plan to export this information, consider using the Show/Hide Columns feature on the console page to add all columns to the table. This assures that all potentially useful information about a threat event is included in the export.

To export threat events to a CSV file, set up the table with the view, columns, and Max Time value you want and then click **Export to CSV**.

## Threat Views on the Files Pages

In addition to Events page views that display events associated with ATIs and other threat monitoring, the Files pages provide views that report on the existence of suspicious or threatening files, even if they were created prior to the installation of the Bit9 Agent on an endpoint.

To view the Files pages, choose **Assets > Files** on the console menu and choose the tab for either **File Catalog** or **Files on Computers**. The following threat-related Saved Views are available on these tabs:

- **Threat Report - Suspicious Files by Extension** (File Catalog only) – This view identifies files that have been analyzed and determined to be executables by Bit9 but have an extension that is not an executable type. Malware often tries to disguise itself by using normally benign file extensions such as “.gif” or “.jpg”.
- **Threat Report - Suspicious Files by Name** – (Files on Computers only) This view shows files in the inventory that have names similar to the name of a common file (such as an operating system file), zero trust level in Bit9 SRS, and a File State of Unapproved.

As with Event views, you can click on the **Show/Hide Filter** button on the Files pages to see the extension and other parameters that create these views. The views have the potential to produce many “false positive” results. To reduce the number of results, additional factors such as file trust, size, and publisher are used in this view. You can further modify and save the view under another name to create your own version of a threat report for files.

## Threat-Related Alerts

You can create an alert that is triggered whenever an ATI determines that a potential threat has occurred. Alerts for this purpose are Event Alerts, and can be fine-tuned to included or eliminate certain types of threat events. All Event Alerts must include at least one Subtype in the Select Event Properties panel. In the example below, an alert is being created that used the same properties as the Threat Indicator view on the Events page, and so this event will be triggered any time an event that would be displayed in that view occurs.

Alerts make it easier to monitor specific events, and can be configured to send email to one or more recipients when triggered. See [“Using Bit9 Alerts”](#) on page 494 for instructions on creating and configuration alerts.

## Responding to Threats

If you see a threat that requires remediation or further attention, there are many ways you can respond. A key step before taking action is to research the files, processes, users, and other information included in the report.

Once you determine that a response is required, you might take actions outside of Bit9, such as deleting instances of suspicious files or creating new firewall rules. Within the Bit9 Security Platform, you can check the box next to events reported in threat views and act on the files reported in the events using the commands on the Action menu, including:

- **View Bit9 SRS Cloud Data** – If you have enabled Bit9 SRS, you can open the Bit9 SRS site to view additional information about a file (if available), including its first seen date and prevalence on Bit9-monitored computers.
- **Send Suspicious Files for Analysis** – If you have used the Bit9 Connector to integrate an external analysis appliance or service, you can send files reported as threats for external analysis. Note that this option sends the target file noted in a threat event for analysis, not the process.
- **Ban Globally/Ban by Policy** – You can ban a suspicious or malicious file directly from the Action menu in one of the threat views. Bans should be used carefully since it is possible that a file reported in a threat report is used for both acceptable and

unacceptable purposes. One way to determine this is to begin with a Report Only ban, an option available on the Ban by Policy page.

The screenshot shows the 'Events' page in the Bit9 Security Platform. At the top, there are filters for 'Saved Views' (set to 'Threat Indicators') and 'Group By' (set to '(none)' with 'Ascending' order). Below these are links for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', 'Access Event Archives', and 'Refresh Page'. A dropdown menu for 'Action' is open, listing various actions such as 'Approve Locally', 'Remove Local Approval', 'Approve Globally', 'Ban Globally', 'Approve by Policy', 'Ban by Policy', 'Remove Approval or Ban', 'Upload to Server', 'View Bit9 SRS Cloud Data', 'Analyze with Check Point', 'Analyze with FireEye', 'Analyze with Palo Alto Networks WildFire', 'Create Indicator Set Exceptions', and 'Create Advanced Indicator Set Exception'. Below the menu is a table with two columns: 'Set' and 'Rule Name'. The table lists various system configuration and suspicious file rules.

Set	Rule Name
System Configuration	Windows firewall tampering
System Configuration	Windows firewall tampering
Startup Configuration	Unusual change to startup configuration
Startup Configuration	Unusual change to startup configuration
Suspicious Based on Path and File Name	Suspicious executable based on location
Suspicious Based on Path and File Name	Suspicious executable based on location
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
Suspicious Based on File Name	Suspicious executable based on extension
System Configuration	Possible name resolution tampering

In addition to the choices on the Action menu, there may be situations in which creation of a different type of rule, such as a custom or registry rule, could mitigate the threat. These rules require that you enter their parameters manually. You can copy file, registry, or process information from events in the threat views and then configure the other rule parameters in the way you choose, being careful to restrict the rule to the actions you are certain you want to block or report on to avoid blocking critical files or processes. See [Chapter 12, “Custom Software Rules,”](#) [Chapter 14, “Registry Rules,”](#) and [Chapter 15, “Memory Rules,”](#) for more information about creating these rules.

## Responding to Threats with Event Rules

Bit9 Event Rules allow you to take certain actions when events matching the rule definition occur. This offers an automatic way to respond to threats, even if you haven't reviewed them on the Events page. Although you cannot automatically ban files using event rules, you can take other actions that might be useful for reported threats:

- **Remove Approval from Suspicious Files** – You can use event rules to automatically remove local or global approval from files matching the rule parameters.
- **Send Suspicious Files for Analysis** – If you have used the Bit9 Connector to integrate an external analysis appliance or service, you can create an event rule that sends files reported as threats for external analysis. For example, in the illustration below, files reported in threat events and that are not already banned are sent to WildFire for analysis. This can provide more information that might influence your decision to block or not block a file.
- **Create a Ban** – You can define an event rule that creates a Report Only ban for any file included in a threat event triggered by an ATI. A Report Only Ban will generate an event telling you that a file would have been blocked if the Ban was fully activated.



Although not available by default, the option to create fully functional bans through Event Rules may be enabled with the assistance of Bit9 Technical Support.

The screenshot shows the 'Create Event Rule' dialog box with the following configuration:

- General:**
  - Copy Settings From: (none)
  - Rule Name: Analyze Detected Threat Files (Copy)
  - Description: Send suspicious files detected by ATIs to WildFire.
  - Status:  Enabled  Simulate only  Disabled
- Select Event Properties:**
  - Add filter: [dropdown]
  - Subtype: is [dropdown]
  - Indicator Set: is not empty [dropdown]
  - Report access (memory rule) [dropdown]
  - Report execution (custom rule) [dropdown]
  - Report execution (removable media) [dropdown]
  - Report read (removable media) [dropdown]
  - Report write (custom rule) [dropdown]
  - Report write (removable media) [dropdown]
- Select File Properties:**
  - Add filter: [dropdown]
  - Global State: is not [dropdown]
  - Banned [dropdown]
  - Banned by Policy [dropdown]
- Select Process Properties:**
  - Add filter: [dropdown]
- Select Action:**
  - Action: Analyze file [dropdown]
  - Priority: Medium [dropdown]
  - Use Palo Alto Networks WildFire:

Buttons at the bottom: Create & Exit, Save, Cancel.

See [Chapter 16, “Event Rules,”](#) for more information about creating and editing event rules.



## Chapter 21

# Using and Customizing Dashboards

Bit9 Dashboards are configurable pages containing compact windows called “portlets,” each of which provides access to Bit9-related information or controls.

**Sections**

Topic	Page
<a href="#">Dashboards Overview</a>	568
<a href="#">Using Portlets</a>	570
<a href="#">Changing Dashboard Appearance</a>	576
<a href="#">Creating, Editing and Managing Dashboards</a>	579
<a href="#">Managing the Default Home Page</a>	584
<a href="#">Creating and Customizing Portlets</a>	586

## Dashboards Overview

If you have not changed the default start page, the Home Page dashboard is the first page shown when you log in to the Bit9 Console (if not, click **Home** in the console menu).

The screenshot displays the Bit9 Home Page dashboard with the following components:

- Alerts:** A table showing a 'Backup Missed Alert' of type 'System Alert', enabled, and last modified on 2012-10-06 08:24:22.
- Top X:** Search filters for 'Find top' (10), 'Max age' (Last Day), and 'Blocks by Computer'.
- Find Computer:** Search options for 'Computer name or IP' or 'User name'.
- Find Files or Events:** Search filters for 'Computer' (Any Computer), 'User' (Any User), 'Filename' (All Files), and 'Max age' (Last Day).
- Change Policy:** Interface to change policy for a specific computer.
- Event Reports:** A table showing reports for the period 10/5/2012 1:39 PM to 10/6/2012 1:39 PM.
 

Report	Files	Computers
<a href="#">New installations</a>	256	31
<a href="#">New unapproved files</a>	1567	31
<a href="#">Blocked files (by bans)</a>	210	14
<a href="#">Blocked files (by unapproved status)</a>	1005	18
- Licensing:** A table showing license usage.
 

License Type	Limit	In Use
Visibility	0	0
Control	40	31
- Emergency Lockdown:** A button to move all connected computers not under High Enforcement Level to High Enforcement Level.

A Dashboard consists of a series of *portlets*, each of which provides summary information or controls that can help you manage the security of your computers and the files on them. Some portlets display a specific type of information from your Bit9 database, such as events or baseline drift. Others might display news feeds or other information from an outside URL.

**Note**

This chapter uses the Home Page as an example for explaining dashboard features. For a complete list and description of the Home Page portlets, see [Table 2, “Home Page Quick Access Portlets”](#) on page 51.

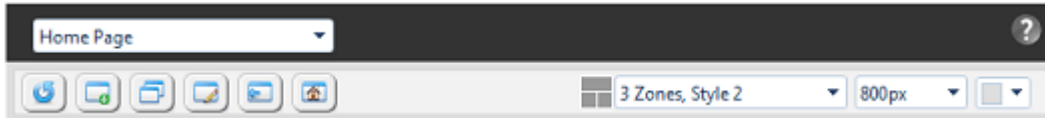
- The initial section of this chapter describes basic elements of a dashboard and how to use them. If you intend only to use Bit9-provided dashboards as they were delivered, this is the only section you need to read.
- The second major section of the chapter describes customizing the *appearance* of a dashboard. If you plan to use only existing dashboards but would like to change some aspects of the way they are displayed, this section will help you accomplish that.
- The third major section of the chapter describes how to create and customize dashboards and the information and controls on them. This includes choosing to share a dashboard with other users.
- The final section of the chapter describes how to create and edit the portlets that make up a dashboard.

What you can do with dashboards depends on the privilege level of your console login account – the descriptions below assume default permissions for each group:

- Administrators and PowerUsers can view, use the features of, create, change, and delete their own dashboards and dashboards shared by other users. They can share dashboards they create, and they can choose a different default Home Page for new users of your Bit9 Console.
- Administrators and PowerUsers can view, use the features of, create, change, and delete portlets.
- ReadOnly users can access and use the features of their own dashboards, Bit9-provided dashboards such as the Home Page and System dashboard, and any dashboards other users have created and shared. They can create, change, or delete their own dashboards. They cannot modify or delete other dashboards, share dashboards they create, or choose a different default Home Page for new Bit9 Console users.
- ReadOnly users can view and use the features of portlets except for those that access features they do not have permission to use, such as Emergency Lockdown and Changing Policy for a Computer. They cannot create, modify, or delete portlets.
- You can enable or disable permissions for dashboard access by using the Manage Shared Dashboards checkbox on the Group Details page (see [“Managing Console Account Groups”](#) on page 89).

## Dashboard Elements

Although the portlets displayed by a dashboard vary, the basic structure of all dashboard pages is standard. The two main areas are the Dashboard toolbar, which shows the name of the current Dashboard and provides buttons and menus to manage it, and the portlets.



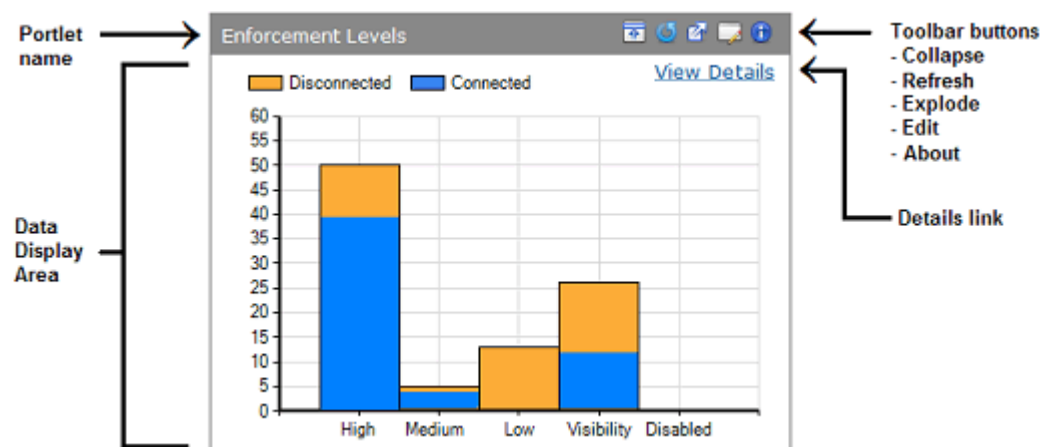
The dashboard toolbar includes:

- Current dashboard name – This appears at the top left of the toolbar.
- Dashboards menu – Clicking on the down-arrow next to the dashboard name opens the dashboards menu, which allows you to choose a different dashboard to display.
- Dashboard Help button – The question mark button in the upper right area of the dashboard page opens general help about dashboards. For each individual portlet, an information button in the upper right corner provides a description of that portlet.
- Dashboard action buttons – The Reload button reloads the current dashboard. The remainder of the buttons are used for more advanced activities described in the section “[Creating, Editing and Managing Dashboards](#)” on page 579.
- Dashboard appearance option menus – These options, on the right half of the toolbar, are described in detail in “[Changing Dashboard Appearance](#)” on page 576.

## Using Portlets

The portlets on a dashboard may display file, computer, or event information. They might show the number and types of computers managed by Bit9 Agents, the number and type of security policies enforced, or the categories of software on your computers. The dashboard might also include portlets that allow you to make inquiries, such as finding an event or file, or portlets that take actions, such as locking down all computers.

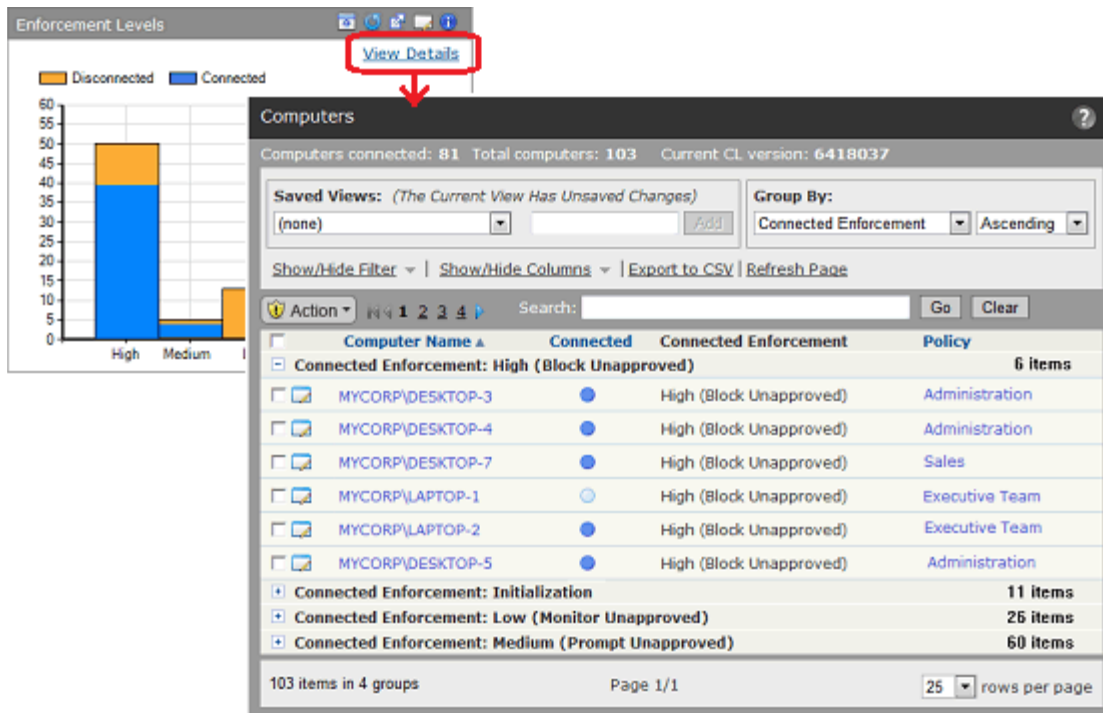
Each portlet has a toolbar with its name in the top left and a series of buttons in the top right. The main content of the portlet is below the toolbar. Data is displayed in this content area in the form of tables, charts, graphs, RSS crawls, or HTML pages. For portlets that take action or allow queries, there are fields to fill in or buttons to click to execute an action. You might also add portlets with other means of conveying data.



In many portlets, moving the mouse cursor over an element of a chart, for example, a bar in a bar chart, provides a description of that element, such as how many computers are represented by a particular bar in the chart.

## Getting More Detailed Data

In addition to displaying key information at their top level, many portlets provide a way to “drill down” for more detail. You get more detail by clicking on graphics or data in a portlet (where the mouse cursor changes into a hand shape) and/or clicking on the **View Details** button, if it is available in the portlet. The first level of detail below the dashboard might be a Bit9 Server page with the additional information about what the portlet shows. Depending upon the portlet, information on the details page might be grouped by the data type shown in the portlet (e.g, computers grouped by Enforcement Level).









To return to a dashboard from a “drilldown” to details, choose the name of the dashboard you were on from the console Home menu. Note that using the back button to return to a dashboard could produce unpredictable results.

## Portlet Toolbar Buttons

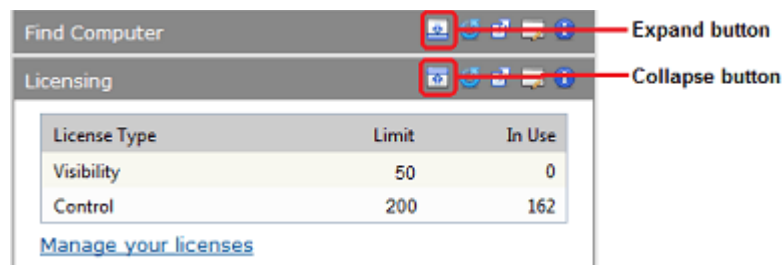
The portlet toolbar offers a variety of options, some of which change the display of a portlet. [Table 89](#) shows the buttons in the toolbar and the actions they take.

**Table 89:** Portlet Toolbar buttons

Button	Description
 Collapse	Collapse the view of the portlet so that only its toolbar is displayed.
 Expand	Restore a collapsed portlet to its normal display.
 Reload	Reload the portlet with the most current data available.
 Explode	Explode the view of the portlet so that it covers the entire dashboard. Clicking the X in the upper right corner of an exploded portlet restores it to its normal size.
 Edit	Open the Portlet Details page for this portlet, which provides access to editable parameters. What can be edited varies by portlet type and source. For some portlets built-in portlets, the only editable parameters are the name and the description that appears when a user clicks the information button. See <a href="#">“Editing Portlet Details”</a> on page 587.
 Information	Open the information window for this portlet, which provides a brief description of the purpose of the portlet and how to use it. This information may be edited.

## Collapsing, Expanding, and Exploding Portlets

There are two features for changing the way portlet windows are displayed on a dashboard. One allows you to “collapse” a portlet to display its name and toolbar only, and then to “expand” the portlet back to its normal state. The Collapse or Expand button (depending upon the current portlet state) is in the toolbar on the right side of each portlet.



Exploding a portlet is a temporary viewing option that allows you to take over the entire dashboard display area with one portlet. When you are finished with the exploded view, click the X button in the top right area of the portlet to return to normal viewing.

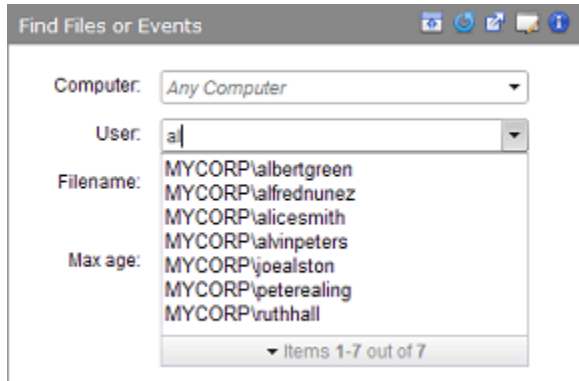
The size of an “exploded” portlet depends upon the size of the Bit9 Console browser window at the time the explode button was clicked.

## Entering Information into Portlets

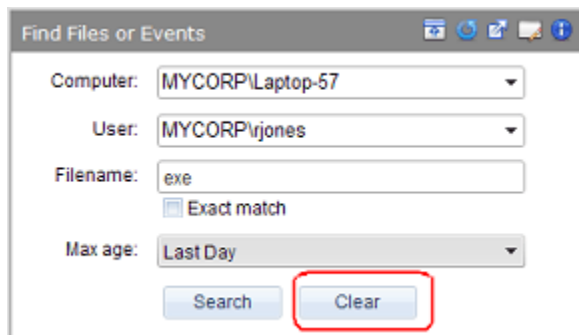
The Bit9 Security Platform is shipped with System portlets, not all of which are on the original Home Page. Some System portlets provide fields for entry of data, such as a computer name, a file name, or a user name, in order to conduct a search for information or to take an action on the item identified in the data. These portlets have several useful features.



Where you type in the name of something stored in the database for your Bit9 Server, a portlet provides an “auto-complete” feature – as you type, a list of possible matches to what has been typed so far is displayed in a menu. If the item you are looking for appears in the menu, you can simply point and click it to finish entering the name. As the example below shows, auto-complete matches what you have typed with any object in the category you chose (*User* in the example) that *contains* the string, not just those that begin with it. Note, however, that you can choose an *Exact match* option for Filename rather than the default behavior of finding every file containing the entered string.



When you enter data into a portlet, the data you enter generally stays in the fields (i.e., becomes the default) unless you change it. This can be helpful if you want to do multiple searches (or other actions) with most but not all of the same information you first entered. To start over with no data on the portlet, click the **Clear** button.



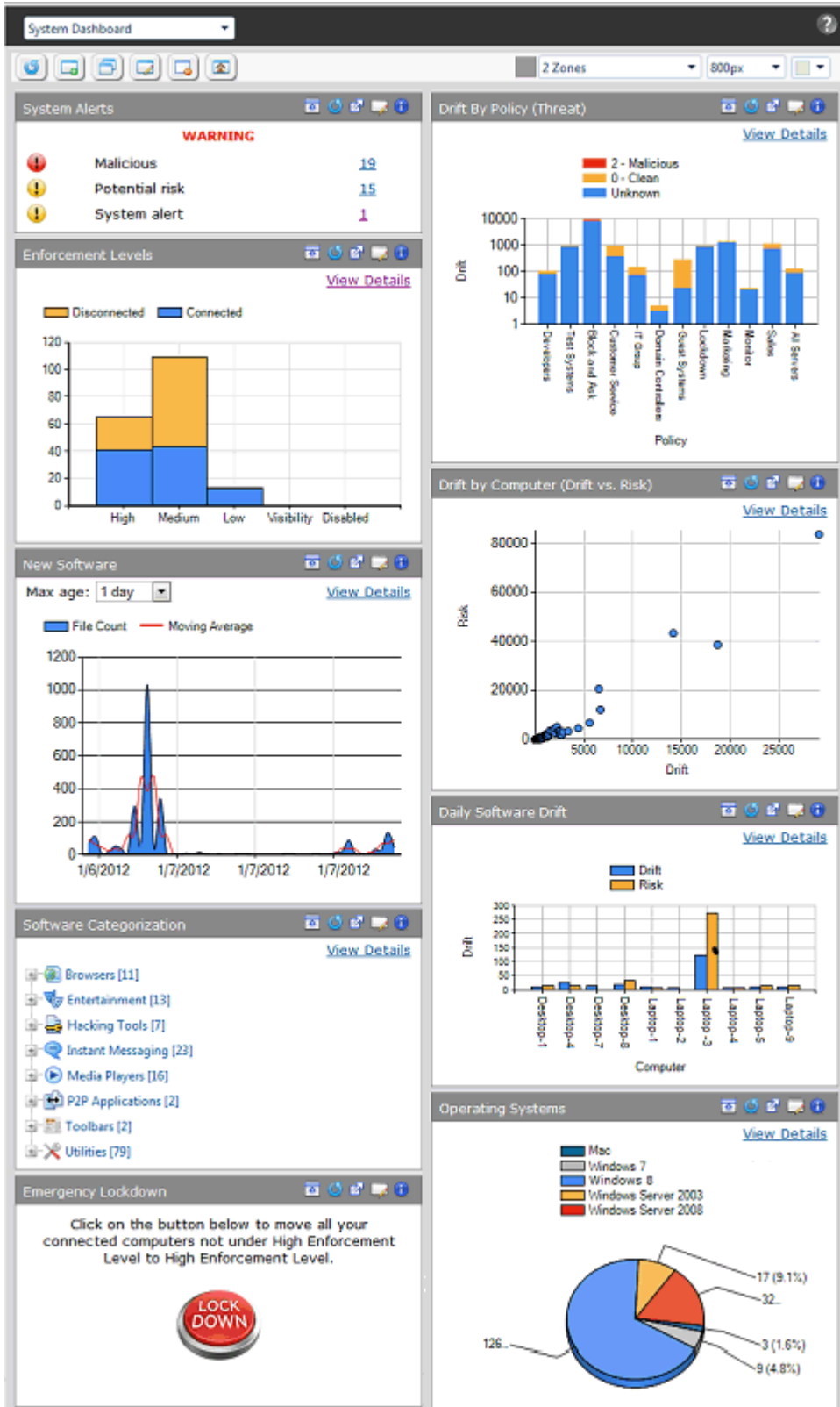
## Other Portlet Controls

Portlets can have special controls that provide more information or take an action. For example, the Emergency Lockdown portlet has large buttons for Lockdown and Restore. The Alerts portlet has highlighted text links for resetting some or all links. Where there are special controls, text in the portlet itself should make their purpose clear.

## Viewing Other Dashboards

The Home Page is always available on the Bit9 Console menu. In new installations of Bit9 (Parity) 6.0 or later, there also is a *System* dashboard with portlets showing a variety of reports on your system, including the number of computers at each Enforcement Level, new software seen on your system, and baseline drift reports. Upgrades to Bit9 v7.2.1 from a previous release may include other dashboards available created in the previous version.

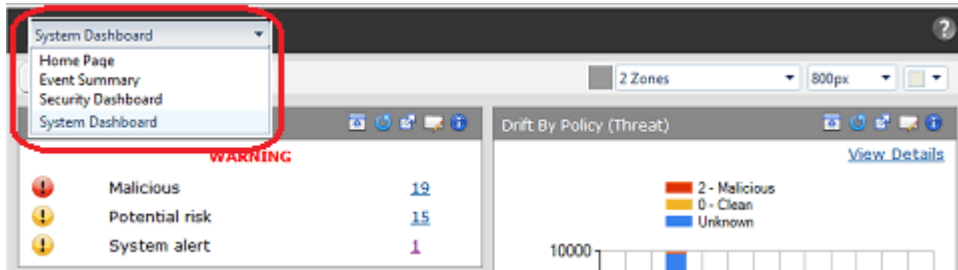
The illustration below shows the type of portlets on the System dashboard (your System dashboard might have more, fewer, or different portlets).



There are several ways to choose and open a different dashboard.

**To open a dashboard:**

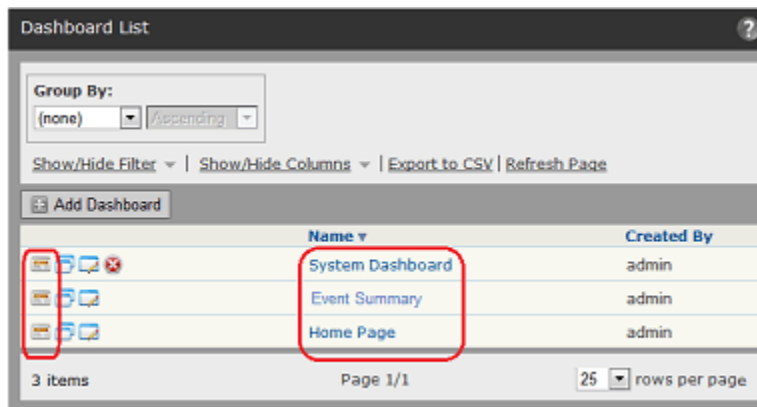
- If you are on a dashboard, choose a different one from the menu in the top left of the toolbar:



- Or, from any console page, move the cursor over **Home** in the console menu to view other dashboard choices. Note that not all dashboards are necessarily added to the menu.



- Or, choose **Reports > Dashboards** on the console menu and on the Dashboard List, either click on the View Dashboard button next to a dashboard name or click on the name itself.



## Changing Dashboard Appearance

The following options can be used to change the appearance of a dashboard:

- changing the layout of portlets on the dashboard
- changing the dashboard width
- changing the dashboard background color
- collapsing and expanding portlet windows
- moving portlets on the dashboard

Three of these options are on the menus on the right half of the toolbar:

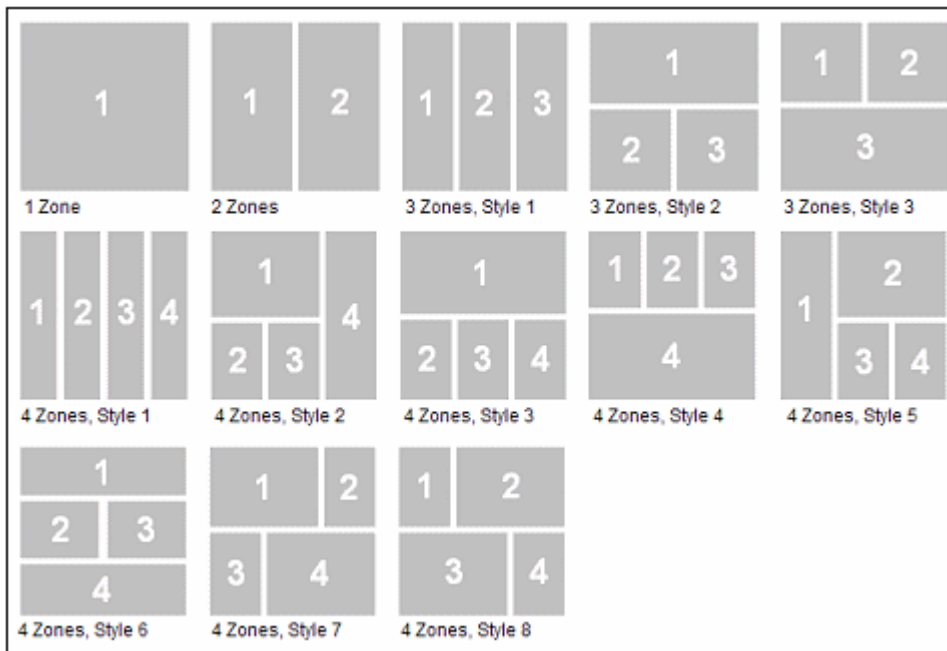


Note that this section describes what can be done to change the appearance and layout of an existing dashboard with existing portlets. Adding and removing portlets is described in the section “[Editing a Dashboard](#)” on page 583.

These appearance options affect only the current dashboard, and are specific to the currently logged in user.

## Changing Dashboard Layout

The Dashboard Layout menu shows the current dashboard layout and allows you to select a different layout from a set of 13 templates. The templates create *zones* in which portlets are placed, and in some layouts, these zones have different widths. Once you choose a layout, you can move portlets from zone to zone so they have width appropriate for their content.



Layouts are labeled with the number of zones and the “style” number if there is more than one style with that number of zones. The default layout is two equal columns, which is the only “2 Zones” layout. The number of zones is not the number of portlets – each zone can and usually will have multiple portlets in it.

## Portlet Distribution in Layouts

When you switch between layouts or add portlets, portlets are assigned to zones based on the following rules:

- If you switch to a layout with the same or more zones as your current one, portlets will remain in their assigned zone. For example, if you switch from “2 Zones” to “3 Zones, Style 1,” all of the portlets in zone 1 will remain in zone 1 and all of the portlets in zone 2 will remain in zone 2 until you move them. There is no attempt to map portlets that are in wide zones in one layout to wide zones in a different layout.
- If you switch to a layout that has fewer zones than the current one, portlets will be remapped to new zones. Portlets from even-numbered zones in the former layout will go to even zones in the new, and odd to odd, except when going to the one-zone layout, where all portlets go to the single zone.
- When you add portlets to a dashboard, they are distributed sequentially to each zone, starting with zone one. So if you add three portlets during one editing session, one each goes to zones 1, 2, and 3.
- The console “remembers” the distribution of portlets in layouts you have used. If you change layout and then return to one you used previously, the portlets should appear in the same locations they did before, assuming you have not added or removed portlets.

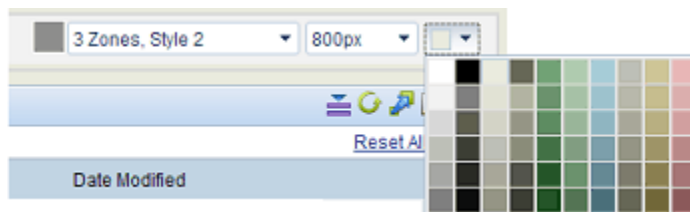
In many cases, you will want to rearrange portlets after a layout change.

## Changing Dashboard Width

The Dashboard Width menu shows the current dashboard width in pixels and allows you to select a width between 600 and 1700 pixels. When you change dashboard width, the width of portlets is resized proportional to their zone within the current layout. Choose a width appropriate to your screen size and resolution, and to the amount of the screen you want to allocate to the Bit9 Console. The default dashboard width is 800 pixels.

## Changing Dashboard Background Color

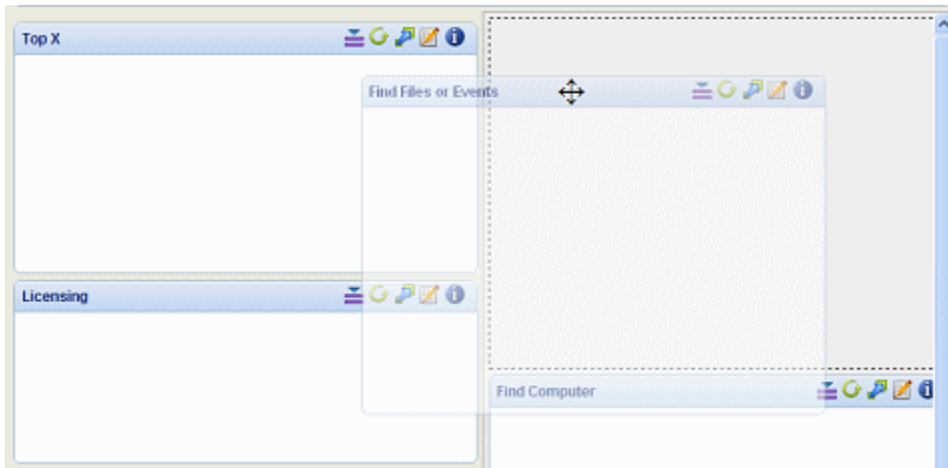
On the Dashboard Color menu, you can change the background color of a dashboard. Clicking on the menu brings up a palette, and clicking a color on the palette makes the color change. The background color change does not affect portlet color. The default background color is light gray.



## Moving Portlets

You move a portlet by clicking in its toolbar and moving the mouse while holding the left mouse button down. When you move a portlet, the portlet you are moving becomes transparent, and only the borders of the other portlets are shown. As you move the portlet, the location in which it would be dropped if you released the mouse button is shown as a dotted-line box, a landing area. If you move from one layout zone into another, the landing

area box shows you any change in portlet width due to the move. When you drop the portlet into its new location, all of the portlets return to normal display.



## Creating, Editing and Managing Dashboards

This section describes the creation and editing of dashboards as well as other dashboard management tasks. Dashboards are defined by the following basic parameters:

- name
- portlets you want on the dashboard
- whether this dashboard will be shared with other users
- whether this dashboard will be listed on the Bit9 Console menu

You can create a new dashboard from scratch or copy an existing dashboard to a new name, modifying it once copied. Whether you are creating, copying, or editing a dashboard, you enter or edit the basic configuration information on the Edit Dashboard page. The main difference among these cases is what information, if any, is filled in for you on the Edit Dashboard page when you start.

In addition to creating and editing dashboards, you might want to:








- set or reload the default dashboard, which is described in [“Managing the Default Home Page”](#) on page 584
- delete dashboards, described in [“Deleting a Dashboard”](#) on page 584

### Note

This section describes how you define and manage a dashboard and its *content*. Ways to customize the *appearance* of a dashboard are described in the section [“Changing Dashboard Appearance”](#) on page 576.

You can access most of the dashboard management tasks described here from either the Dashboards list page or from the toolbar on an individual dashboard. See [“Managing Dashboards from the Dashboards Page”](#) on page 585 for a summary of Dashboards list page features. [Table 90](#) shows the actions taken by the buttons on the dashboard toolbar.

**Table 90:** Dashboard Toolbar buttons

Button	Description
 Reload	Reloads the dashboard and its portlets with the most current data available.
 New Dashboard	Opens the Edit Dashboard page, where you can enter a name for a new dashboard and choose whether to make it available to other users and whether to show it on the console menu (under <i>Home</i> ). You also choose portlets for the dashboard from this page, and can create new portlets using the <b>New Portlet</b> button.
 Copy Dashboard	Opens the Edit Dashboard page for the current dashboard, with all of the current portlets checked for inclusion and a new dashboard name in the form “Copy of <the dashboard you were on>”. You can modify the name as you choose. Saving a copy of a dashboard can be useful if you want to have your own version of a shared dashboard, or if an existing dashboard has some of the portlets you would like to use but you want to add or remove portlets to make it exactly what you need. This also gives you options to add the dashboard to the console menu and share it with all users.
 Edit Dashboard	Opens the Edit Dashboard page so you can modify the current dashboard, including creating new portlets or changing the portlets displayed.
 Delete Dashboard	Deletes the current dashboard (after you choose OK in a confirmation box). See “ <a href="#">Deleting a Dashboard</a> ” on page 584. Not available on the Home Page.
 Reset to Default	Resets a system-provided dashboard (currently, the Home Page and System dashboard) to its currently saved default settings (see Set as Default below). Not available for user-created dashboards.
 Set as Default	Sets the current dashboard as the default Home Page for users whose accounts are created <i>after</i> this setting is saved. See “ <a href="#">Managing the Default Home Page</a> ” on page 584.

## Shared Dashboards

You can create dashboards strictly for your own use only, or you can share any dashboard you create by checking the *Share with all users* box on the Edit Dashboard page.


When dashboards are shared, console users in Administrator or PowerUser groups, or in custom groups with *Manage Shared Dashboards* permission, can modify the dashboard, and they also can delete it.

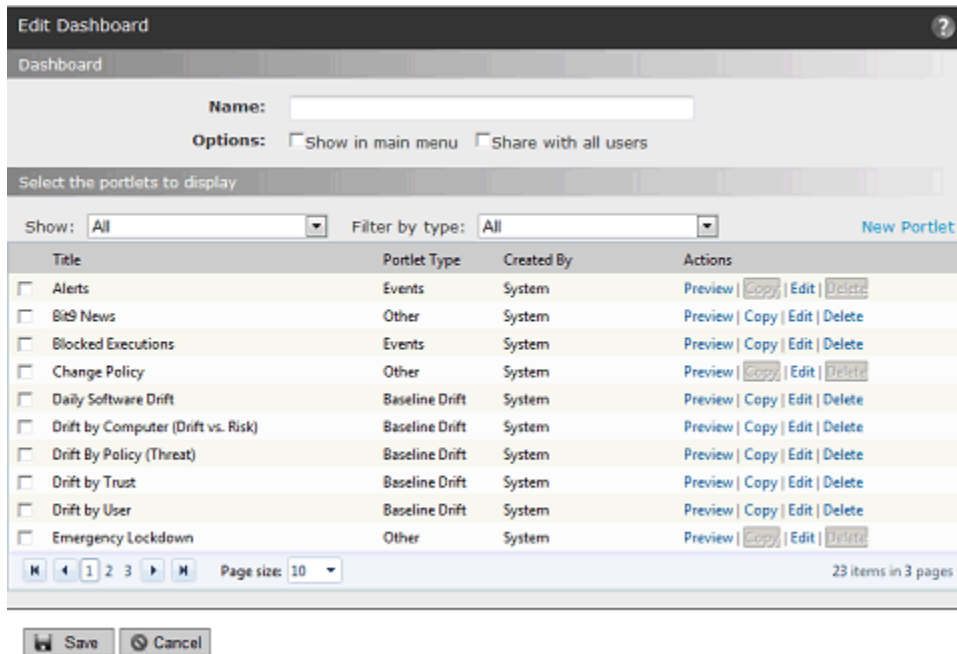
Keep in mind that other users might come to rely on a dashboard you share. If you turn off sharing for a dashboard or delete the dashboard, other users will lose access to it, either immediately, or, if they are on the dashboard, as soon as they navigate away from it.



## Creating a New Dashboard

To create a new dashboard:

1. Open the Edit Dashboard page for a new dashboard using one of the following:
  - Choose **Reports > Dashboards** on the console menu, and on the Dashboards page, click the **Add Dashboard** button.
  - *- or -*
  - On any dashboard, click the Create New Dashboard button .



Title	Portlet Type	Created By	Actions
<input type="checkbox"/> Alerts	Events	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Bit9 News	Other	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Blocked Executions	Events	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Change Policy	Other	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Daily Software Drift	Baseline Drift	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Drift by Computer (Drift vs. Risk)	Baseline Drift	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Drift By Policy (Threat)	Baseline Drift	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Drift by Trust	Baseline Drift	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Drift by User	Baseline Drift	System	Preview   Copy   Edit   Delete
<input type="checkbox"/> Emergency Lockdown	Other	System	Preview   Copy   Edit   Delete

2. In the Name box, enter the name you want for the new dashboard. This is the name that will appear in the upper left when you display this dashboard, and is also the name that will appear on the list of dashboards on the Dashboards page.
3. If you would like to add this dashboard to the Home section of the console menu:
  - a. In the Options line, check the *Show in main menu* box. Note that even if you do not check this box, the dashboard will be available through the Dashboards page and on the Dashboards menu of any other dashboard.
  - b. If you want a different (usually shorter) name to appear on the menu than the one you chose for the dashboard, enter it in the Menu name field, which appears when you check the Show box.
4. If you want other users to be able to use this dashboard, check *Share with all users*.
5. Check the box to the left of each portlet you want to add to this dashboard. Use the page buttons at the bottom of the portlet list or the filters at the top of the list to view all of the available portlets of interest.
 

**Note:** To see what the portlet looks like before adding it to the dashboard, click **Preview** to the right of the portlet name.



6. If you need a portlet not available on the list, see [“Creating and Customizing Portlets”](#) on page 586. Once the new portlet is created, check the box next to its name to add it to this dashboard.
7. Click **Save**. The new dashboard is saved and added to the list on the Dashboards page. If you checked the appropriate box, its name appears on the Home menu on the console menu.

## Copying a Dashboard

Copying a dashboard can be useful under a number of circumstances, including:

- if you want your own copy of a shared dashboard created by someone else
- if you find a dashboard that is close to what you want but would like to add or remove portlets or otherwise edit it for your needs

### To save an existing dashboard under another name:

1. Open the Edit Dashboard page for a copied dashboard using one of the following:
  - Choose **Reports > Dashboards** on the console menu, and on the Dashboards page, click the  button next to the dashboard you want to copy.
  - *- or -*
  - On the dashboard you want to copy, click the Copy Dashboard button .
2. The Edit Dashboard page opens with all of the same parameters as the dashboard you copied, except for the name, which appears in the form “Copy of <name-of-dashboard-you-copied>”. Replace the default “Copy of” name with the name you want to use for the dashboard.
3. Modify any of the other dashboard parameters you would like to change. See [“Creating a New Dashboard”](#) on page 581 for details.
4. Delete any portlets you do not want to appear on this dashboard by un-checking the box to the left of their names.

### Caution

Do not click the Delete link to the right of the portlet name – this deletes it from the Bit9 Server entirely, not just from the current dashboard.

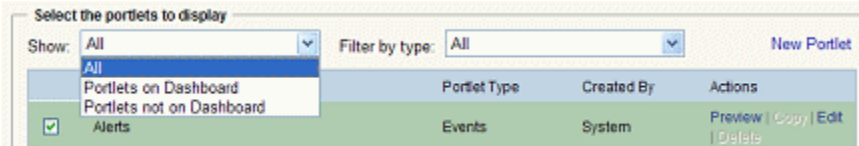
5. Add any portlets you would like to appear on this dashboard by checking the box to the left of their names.
6. If you need a new type of portlet, see [“Creating and Customizing Portlets”](#) on page 586. Once the new portlet is created, check the box next to its name to add it to this dashboard.
7. Click **Save**.  
The copied dashboard appears on the Dashboards page under its new name with whatever modifications you made.

## Editing a Dashboard

You can edit a dashboard to add or remove portlets from it, change its name, or change its sharing and menu options.

### To edit a dashboard:

1. Display the dashboard you want to edit.
2. Click the *Edit this dashboard* button (pencil) in the dashboard toolbar. The Edit Dashboard page appears.
3. Modify any of the dashboard parameters you would like to change, including:
  - a. Portlet name
  - b. *Show in main menu* choice
  - c. *Menu name* (if the *Show in main menu* box is checked)
  - d. *Share with all users* choice
4. On the Edit Dashboard page, the portlet list includes all portlets, including those already on the current dashboard. There are several options for filtering the list:
  - a. If you want to see a list of only those portlets *not* currently on this dashboard, on the *Show* menu choose **Portlets not on the dashboard**.





- b. To see only certain *types* of portlets in the list, choose the type on the *Filter by type* menu; for example, you might choose to show only Computer portlets. See [“Portlet Types and Subtypes”](#) on page 586 for a description of portlet types. You can combine choices on the *Show* menu with choices on the *Filter* menu. Also, these menu choices affect what appears on the Edit Dashboard page, not what appears on the dashboard.
  - c. Whether the list is complete or filtered, if it includes multiple pages, you can click the page numbers or arrows at the bottom of the list to navigate from page to page. The legend in the bottom right corner of the list tells you how many items and how many pages are in the current list.
5. You can use the **Preview** button next to any portlet in the list to see what it will look like on the dashboard.
6. Check the box to the left of the name of each portlet you want to add to the dashboard. See [“Creating and Customizing Portlets”](#) on page 586 if you need to create a portlet not currently found in the list.
7. Un-check the box next to the name of each portlet you want removed from the dashboard.
 

**Note:** Do not click the Delete link to the right of the portlet name – this deletes it from the Bit9 Server entirely, not only from the current dashboard.
8. When you have checked all the portlets you would like to add, click the **Save** button. The dashboard is redisplayed with the new portlets added.

9. If you need to change the overall dashboard layout to accommodate the new portlets, use the Dashboard Layout menu to make this change. See [“Changing Dashboard Layout”](#) on page 577 for more details.
10. If necessary, move portlets on the dashboard to accommodate the new portlets. If you do not know how to move portlets, see [“Moving Portlets”](#) on page 578.

## Managing the Default Home Page

There are two Home Page management buttons on the dashboard:

- Using the Reset to Default button , any user can choose to reset their current, possibly modified, Home Page, to the default Home Page.
- Using the Set as Default button , any user with Administrator or PowerUser privileges (or custom Manage Shared Dashboards permission) can save the current dashboard as the default Home Page for new users.

If you set a different default Home Page, that page becomes the Home Page for anyone using the Reset to Default button. It also is the default Home Page for any new console users who log in for the first time *after* the change to the default. Users who have already logged in before the default Home Page is changed retain their existing Home Page unless they click the Reset to Default button and have permission to make the change.

### Note


To be certain you can go back to the original Home Page, before you (or anyone else) make any modifications, you can use the Copy Dashboard command to copy the Home Page, and rename the copy so that you will have a backup. If needed, you can use Set as Default to restore the Home Page from the backup.

## Deleting a Dashboard

You can delete any dashboard you created and (unless you are logged in as a ReadOnly user) any shared dashboard made available to you. The only dashboard that cannot be deleted by anyone is the Home Page.

When you choose to delete a shared dashboard, a dialog box warns that the dashboard is shared and allows you to confirm or cancel the deletion. Be careful when deleting a shared dashboard since it is possible that other Bit9 Console users want to continue using it. If another user is using a dashboard *when* you delete it, the dashboard remains displayed until they navigate away from it, at which point it becomes unavailable

### To delete a dashboard:

1. Start the deletion process in one of the following ways:
  - On the console menu, choose **Reports > Dashboards** and on the Dashboards page, click the Delete (x) button next to the name of the dashboard to delete.  
*- or -*
  - On the dashboard you want to delete, click the Delete Dashboard  button.
2. In the confirmation dialog that appears, if you are certain you want to delete this dashboard, click **Yes**. The dashboard is deleted and if you were on the dashboard when you deleted it, it is replaced by the Home Page.

## Managing Dashboards from the Dashboards Page

The Dashboards page includes a complete list of available dashboards and controls to manage them. Many of the procedures described in other sections of this chapter reference the Dashboards page for alternative ways to accomplish a task.

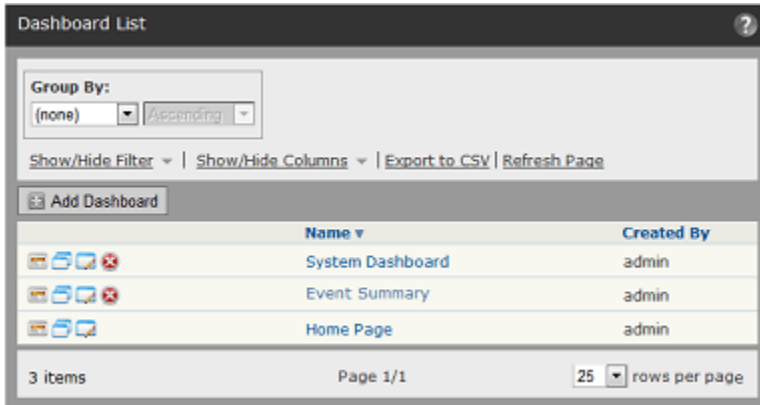






Table 91 shows the dashboard-specific actions available on this page – see also Table 90 for similar commands available when you are already on a dashboard:

**Table 91:** Dashboard List buttons and links

Button/Link	Description
<b>Add Dashboard</b>	Opens the Edit Dashboard page, where you can enter data for creating and configuring a new dashboard. See <a href="#">“Creating a New Dashboard”</a> on page 581 for more details.
 View Dashboard	Clicking this button displays the dashboard in this row. See <a href="#">“Dashboards Overview”</a> on page 568 for an overview.
 Copy Dashboard	Copies the portlets and other settings for the current dashboard to a new dashboard named “Copy of <current-dashboard>”, and opens the Edit Dashboard page. You can modify the name as you choose. Saving a copy of a dashboard can be useful if you want to have your own version of a shared dashboard, or if an existing dashboard looks like a good template. See <a href="#">“Copying a Dashboard”</a> on page 582 for more details.
 Edit Dashboard	Opens the Edit Dashboard page for the dashboard in this row so you can modify the dashboard, including creating new portlets or changing the portlets displayed. <a href="#">“Editing a Dashboard”</a> on page 583 for more details
 Delete Dashboard	Deletes the dashboard in this row (after you choose OK in a confirmation box). See <a href="#">“Deleting a Dashboard”</a> on page 584 for more information. Not available on the Home Page.
Dashboard Name link	Clicking a dashboard name in the list displays the dashboard.

## Creating and Customizing Portlets

In addition to its dashboard management features, the Edit Dashboard page provides access to portlet management features with which you can:

- edit an existing portlet
- create a new portlet
- copy an existing portlet and modify it
- delete a portlet

Any user with Administrator or PowerUser privileges, or in a custom group with dashboard management permission, can use these features. All changes to portlets, including creation and deletion, affect all Bit9 Console users – there are no “private” portlets.

### Portlet Types and Subtypes

Portlets are organized by *types* and *subtypes*. Depending upon the type and subtype, the portlet has different capabilities, and there are different input parameters available when you create or edit it. The types are:

- **Events:** These portlets display event information from the Bit9 database, such as the number of blocked file executions over a period of time or alerts that have been triggered.
- **Baseline Drift:** These portlets display the results of baseline drift analysis, such as daily drift of software from a baseline or a list of the computers with the greatest deviation from the baseline.
- **Computers:** These portlets display information available from the Bit9 Server about the computers on your system, such as the number of computers running each operating system or the number of computers at each Enforcement Level.
- **Files:** These portlets show information about the files on agent-managed computers, such as the number of newly seen files over time or the category (browsers, utilities, messaging, etc.) of the files on the system.
- **Other:** These portlets may display an RSS feed or information from another URL, or they may display HTML pages you provide. This category also includes one-of-a-kind system-created "action" portlets such as the emergency lockdown button, or combinations of different types of information from your Bit9 database.

### System Portlets

The Bit9 Console is installed with a large number of pre-configured portlets. Some of these are visible on the Home Page and might also be on other dashboards at your site. They can be identified by the name “System” in the “Created By” column on the Edit Dashboard page.


Some System portlets, such as the Emergency Lockdown portlet or the Change Policy portlet, are designed to be one-of-a-kind, and cannot be copied or deleted (the Copy and Edit links will be grayed out in their rows). The only changes allowed for these portlets are to their names and descriptions.

## Editing Portlet Details

You can edit portlets to change their appearance or the data presented. You might, for example, decide that a pie chart better presents the data you want to see than a vertical bar chart. The Portlet Details page, where you edit portlets, can be opened from a currently displayed portlet on a dashboard or from the portlet list on the Edit Dashboard page.

See “[Creating Custom Portlets](#)” on page 588 for more detail on the individual parameters you can edit.

### To edit a portlet on the currently displayed dashboard:

1. Click on the Edit button  in the upper right of the portlet you want to edit. The Portlet Details page appears.
2. Make whatever changes you want to the settings on the Portlet Details page. If necessary, click the **Show Advanced Details** button for more editing options.
3. Use the **Preview** link at the bottom of the page to view the effects of your changes. Note that you might need to scroll the browser window down to see the Preview panel. When a preview is showing, you can continue to make changes and click **Refresh** to see the results. Click **Close** when you are finished with the preview.
4. When you are satisfied with the changes you have made, click **Save** at the bottom of the Portlet Details page. The current dashboard appears and shows the portlet with whatever changes you made.

You also can edit portlets via the Portlet Catalog, whether or not the portlet appears on any of your dashboards.

### To edit any portlet from the Edit Dashboard table:

1. On the Edit Dashboard page, find the portlet you want to edit.
2. In the list of portlets, click the **Edit** link to the right of the name of the portlet you want to edit. The Portlet Details page appears.
3. Edit as described in the previous procedure.

## Deleting Portlets

### Caution

Console users in the Administrators group or custom groups with permission to manage dashboards can delete portlets from the Edit Dashboard page (except for certain System portlets). Use this capability with care, since it deletes the portlet from *all dashboards for all users*.

**To permanently delete a portlet:**

1. From any dashboard or the Dashboards page, click the Edit Dashboard (pencil) button. The Edit Dashboard page appears.
2. In the list of portlets, click **Delete** next to the portlet you want to delete. A confirmation dialog appears and includes information about how many dashboards use this portlet. Be sure you actually want to delete this portlet from your Bit9 environment – it will be permanently removed for all users.
3. If you are certain you want to delete this portlet, click **OK** in the confirmation dialog. The portlet is removed from the portlet list on the Edit Dashboard page. It is removed from all dashboards that include it.

If a user is viewing a dashboard containing the portlet, the portlet will remain visible until the user reloads or navigates away from the dashboard.

## Creating Custom Portlets

In addition to making available portlets created by Bit9, dashboards provide the means to create and use your own portlets. You can choose from a list of several portlet types that can present data about your Bit9-managed assets and rules, and then configure the appearance of data from those reports as you choose.

Regardless of who creates a custom portlet, the portlet is available to all console users through the Edit Dashboard page. Note, however, that ReadOnly users cannot create or modify a portlet.

As you enter details for your portlet, don't hesitate to experiment with different settings on the Portlet Details page and click the **Preview** button. The Preview capability serves as both a debugger, to inform you when you choose incompatible settings for a portlet, and a good way to try different charts or different collections of data before adding a custom portlet to a dashboard.

**To create a custom portlet:**

1. Click the Edit Dashboard button, either on a currently displayed dashboard or next to the name of any dashboard on the Dashboards list.
2. On the Edit Dashboard page, click **New Portlet**. The New Portlet page appears.
3. On the New Portlet page, choose the type from the *Select portlet type* menu. See [“Portlet Types and Subtypes”](#) on page 586 for a description of the portlet types.
4. If there is more than one choice, choose the subtype from the *Select subtype* menu.
5. Click **Next**. The Portlet Details page appears. This is the same Portlet Details page that appears when you edit a portlet.

**Note**

The type and subtype of a portlet determine its fundamental structure and many of the available choices on the Portlet Details page. They cannot be edited once chosen. If you want to change type or subtype during the portlet creation process, click **Cancel** and start over.



## Adding Portlet Details

6. On the Portlet Details page, enter the General details, which include the following:
  - a. **Title:** Type the title you want to appear on the portlet and in the portlet list on the Edit Dashboard page.
  - b. **Description:** Type the information you want users to see when they click the information button for this portlet, such as a short description of the purpose of the portlet and instructions for how to use it.
7. If the Portlet Details page includes a panel specific to your portlet type, such as *Baseline Drift details* or *RSS details*, fill in the required information there and then click **Next**.  
If there is a **Save** link instead of a Next link, click it to save the new portlet and add it to the catalog and current dashboard. For some portlet types, no further configuration is necessary.
8. If a Data Presentation panel appears, you have the option of choosing Table as the Chart type.
  - If you choose **Table**, select the columns and column *order* you want, then continue with step 14. See “[Using Tables in Portlets](#)” on page 591 for details on configuring table portlets.
  - If you choose any other Data Presentation type, continue with step 9.
9. If a Graph Settings panel appears on the page, provide the details for the way in which you want the data for this portlet presented. The available choices vary depending upon the type and subtype of portlet, but generally those shown in [Table 92](#).
10. When you finish choosing Graphic Settings, click **Preview** to see what your portlet will look like. You can try a variety of settings, such as different chart types, to find the one you like best. Use **Refresh** to update the preview as you change settings.
11. Once you have specified the basic appearance of the chart for this portlet, you can do one of two things:
  - a. If you do not want to view and modify advanced graphic details, click **Save** to add the portlet to the Edit Dashboard page.
  - b. If you do want to see additional graphic settings, click the **Show Advanced Settings** button.
12. If you are reviewing advanced graphic settings, you have the choices shown in [Table 93](#). Note that not all advanced settings are appropriate (or available) for all chart types.
13. If you have entered Advanced details, you can click the **Preview** link again to examine your portlet before saving.
14. If the Portlet Details page for the portlet you are creating has a filters panel and you want to filter the data that will be used in the portlet (both graphic and table-only portlets), configure the filter you want. See “[Using Filters in Portlets](#)” on page 595 for more details.
15. When you are satisfied with the appearance and data of your portlet, click **Save** to add the portlet to the Portlet Catalog, add it to the current dashboard, and close the Portlet Editor.

**Table 92:** Portlet Graphics Settings

Setting	Description
<b>Chart type</b>	This menu lists the ways you can represent data for the portlet type and subtype you chose. The list may include points, bars, and pie charts, among other choices.
<b>X-axis</b>	This lists the types of attributes available for the portlet type and/or subtype you chose. Choose one (for example, Computer name) to distribute along the X axis of the chart. For different types of charts, the choice here might not determine what appears on the X axis but what is the fundamental data in another format, for example, what each slice of a pie represents.
<b>Limit to the 5 10 15 highest lowest values</b>	If you put certain data, such as individual computers, on the X-axis, you can have too many instances to display effectively inside the portlet. The “Limit to” checkbox and menus allow you to show only the instances with the 5, 10, or 15 highest or lowest values of whatever it is you are displaying (drift, for example). Presumably these would present the most interesting information, and the limit allows you to have a usable graphic rather than putting too much information into too little space. This box is not displayed for certain chart types, including scatter charts or columns using the “auto split” feature.
<b>Group by</b>	Appears only if you choose <b>Scatter</b> as the Chart type. If you choose a <i>Group by</i> value, the dots on the scatter chart represent the total value for the group you indicate rather than values for an individual group member. For example, if you choose Policy as the <i>Group by</i> value, instead of dots representing a Y value for individual computers, they would represent the Y value for all the computers in a policy instead.
<b>Exclude “Unknown” X-axis values</b>	If you check this box, data with unknown X-axis values is eliminated from the chart or graph. This is another way to eliminate less useful information from the portlet.
<b>Split by</b>	Specifies the information type whose values split the X-axis data. For example, you might create a portlet that shows raw drift by policy. <i>Split by</i> creates a separate series (bar, column, or segment) for each unique value in selected column, so a bar representing all the computers in a policy can be split (by color) to show how much drift is attributable to each computer.
<b>Metrics</b>	Lists the choices of attributes you can represent on the Y-axis of your chart. If you can only choose one value for the particular portlet type you are creating, this is a dropdown menu. If you can choose multiple types, this is a multi-select menu that allows you to move more than one item from the <i>Available</i> columns to the <i>Selected</i> column or vice versa. You can add any metrics that are shown as available. For example, for a bar chart of unique files by global state, you could add “Count” to show the number of files in each state and then also add “Prevalence” to show how many computers have files of each type.
<b>Show table below graph</b>	When checked, displays a list of table columns available for this portlet. Move those columns you want displayed into the Selected column. See <a href="#">“Using Tables in Portlets”</a> on page 591 for more details.

**Table 93:** Portlet Advanced Settings

Setting	Description
<b>Height</b>	Allows you to choose a height, in pixels, for the portlet, or to let the dashboard size it for you (Auto). Note that if you choose a value other than <i>Auto</i> , you may interfere with proper display of the portlet.
<b>Show X axis title/ Show axis titles</b>	When box is checked, includes the X-axis title (that is, the title shown in the X-axis box in Graph Details) on the portlet chart, or if X and Y axes are shown, titles for each.
<b>X-axis labels</b>	For choices other than None, adds labels to the data points on the chart (for example, the bars in a bar chart), in the location and orientation you choose. If you choose Auto, the dashboard specifies label positioning based on the best fit.
<b>Legend</b>	When any button but None is clicked, provides a legend describing the chart elements in the location you specify. For example, if different colors are used for total systems vs. connected systems, the legend identifies which is which.
<b>Include tooltips</b>	(Alternative to Legend) When this box is available and checked, hovering the mouse cursor over a chart element displays a tooltip describing what the element represents.
<b>Show Data Point Values</b>	When box is checked, displays the Y values (or their equivalent) on the portlet chart. For example, if a column represents three computers, the number 3 is displayed above the column.
<b>Draw 3D</b>	When box is checked, displays the chart with 3D effects.
<b>Use logarithmic scale</b>	When box is checked, changes the scale for displayed data from linear to logarithmic.

## Using Tables in Portlets

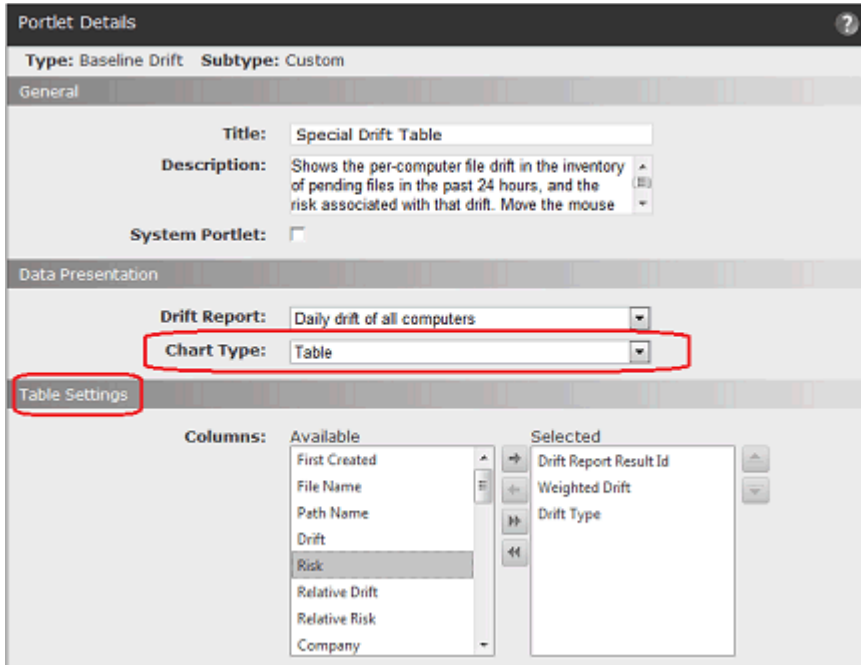
When portlets have content appropriate for display in a table, there are two table options that can appear on the Portlet Details page:

- **Table Only:** The Portlet Details page provides a table option in the *Chart type* menu. This is the option to choose if you do not want any graphic charts on the portlet.
- **Supplemental Table:** If the main chart type choice is something other than *Table*, a *Show table below graph* checkbox appears at the bottom of the Graph Settings panel. When you check this box, you get both a graphic representation and a table.

## Table-only Portlets

Table-only portlets can be a good choice when you would like to display Bit9 data on the dashboard that doesn't lend itself to graphic representation. For example, you might not be interested in *how many* computers or files meet certain criteria but instead in a more complex picture of different kinds of data for each computer, or for each file.

When table-only presentation is possible, a Data Presentation panel appears on the Portlet Details page. In that panel, you can choose **Table** as the Chart type. Choosing this option replaces the Graph Settings panel on the Portlet Details page with a Table Settings panel in which you choose and order the data to include in the table.



You must choose the columns you want to appear in the table. You can double-click on a data element in the Available column to move it to the Selected column, and vice versa. You also can use the arrow buttons to move items back and forth between Available and Selected, and to change the order of data in the table.

Table portlets provide many features for rearranging the data they display:

- You can have multi-page tables and navigate between pages using the page and arrow buttons in the bottom left of the portlet.
- You can determine the number of rows displayed in a table by choosing a different *Page size* (in multiples of 10 rows).
- You can click over a column and drag it to a different location in the table.
- You can click over a column heading and drag it into the labeled zone at the top of the portlet to group the table by the data named in the column heading.
- You can filter the contents of a table by any column head to show data of interest. (You also can pre-filter the data using the Filters on the Portlet Details page.)
- You can click on a column head to sort by the data in that column.

Computer Status

Drag a column header and drop it here to group by that column

Computer Name	Parity Agent Version	Connected	Policy
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Mycorp\Desktop-1	6.0.2.305	True	Domain Controllers
Mycorp\Desktop-4	6.0.2.305	True	Research Group
Mycorp\Desktop-6	6.0.2.305	True	Sales
Mycorp\Desktop-7	6.0.2.305	True	Research Group
Mycorp\Laptop-2	6.0.2.305	False	Executives
Mycorp\Laptop-3	6.0.2.305	False	Research Group
Mycorp\Laptop-4	6.0.2.305	True	Marketing
Mycorp\Laptop-9	6.0.2.303	True	Customer Service
Mycorp\Laptop-10	6.0.2.305	False	Sales
Mycorp\Laptop-11	6.0.2.305	False	Research Group

Page size: 10 167 items in 17 pages

To filter on a column, enter a string in the box below the column – for example, “Laptop” in the Computer Name column, and then click on the filter button to see the operator menu, where you can choose *how* you want to use the string you entered to filter the data.

Computer Status

Drag a column header and drop it here to group by that column

Computer Name	Parity Agent Version	Connected	Policy
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Mycorp\Desktop-		True	Domain Controllers

Operator menu:

- DoesNotContain
- StartsWith
- EndsWith
- EqualTo
- NotEqualTo

## Supplemental Tables in Portlets

You can add a supplemental table within a graphic portlet. Because the space is shared, you probably will not want to create elaborate supplemental tables.

When a supplemental table is possible, a *Show table below graph* checkbox appears at the bottom of the Graph Settings panel. Check this box to display the Table Settings panel.

The screenshot displays the configuration interface for a portlet. It is divided into three main sections:

- Data Presentation:** Contains a 'Chart type' dropdown menu set to 'Column'.
- Graph Settings:**
  - 'X-axis' dropdown set to 'Publisher or Company'.
  - Checkboxes for 'Limit to the 5 highest values' and 'Exclude "Unknown" X-axis values' are checked.
  - 'Split by' dropdown set to 'None'.
  - 'Metrics' section with 'Available' and 'Selected' lists. 'Available' includes File Size (avg), File Size, Prevalence (avg), and Prevalence. 'Selected' includes Count.
  - A checkbox labeled 'Show table below graph' is checked and highlighted with a red box.
- Table Settings:** (This section is also highlighted with a red box)
  - 'Columns' section with 'Available' and 'Selected' lists. 'Available' includes File Id, Date Created, Last Updated, First Seen Name, SHA-256, Global State, Extension, and First Seen Path. 'Selected' includes Publisher or Company and Count.

You must choose the columns you want to appear in the table – your Metrics choices for the Graph Settings are not imported to the table. You can double-click on a data element in the Available column to move it to the Selected column, and vice versa. You also can use the arrow buttons to move items back and forth between Available and Selected, and to change the order of data in the table.

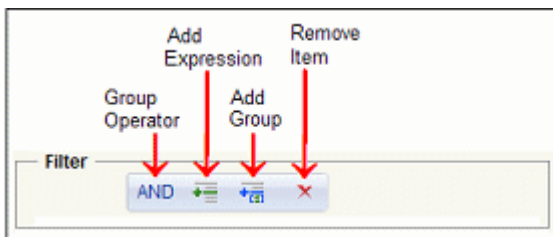


As with table-only portlets, you can drag and drop columns to rearrange them, and can sort data by clicking on column heads. You cannot group by column and cannot filter the data in the table itself.

## Using Filters in Portlets

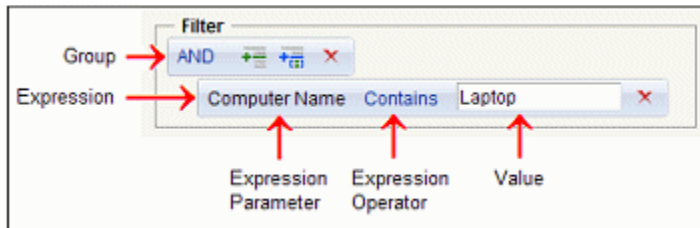
Some portlets allow you to use filters to limit and focus the information a portlet displays. For example, you could create a portlet that shows the connection status of computers but filter out those in Visibility mode policies.

Filters do not make sense for certain portlets – RSS feeds and HTML pages, for example – and are not used on the pre-configured portlets installed with the Bit9 Server. If the portlet you are creating or editing includes a filtering capability, you will see a Filters panel on the Portlet Details page. The illustration below shows the initial building blocks of a portlet filter.



This initial filter view shows the top-level group operator. To have the filter actually do anything, you need to add at least one *expression*, a set of parameters that can be evaluated as true or false against Bit9 data. For example, to have the filter include only those

computers containing “Laptop” in their name in the portlet data, you would create the following filter.



Each expression consists of a parameter--some kind of data that is available in the Bit9 database, an expression operator, and a value. You choose the parameter and operator from menus that vary depending upon that type and subtype of portlet. You type in the value you want to match.

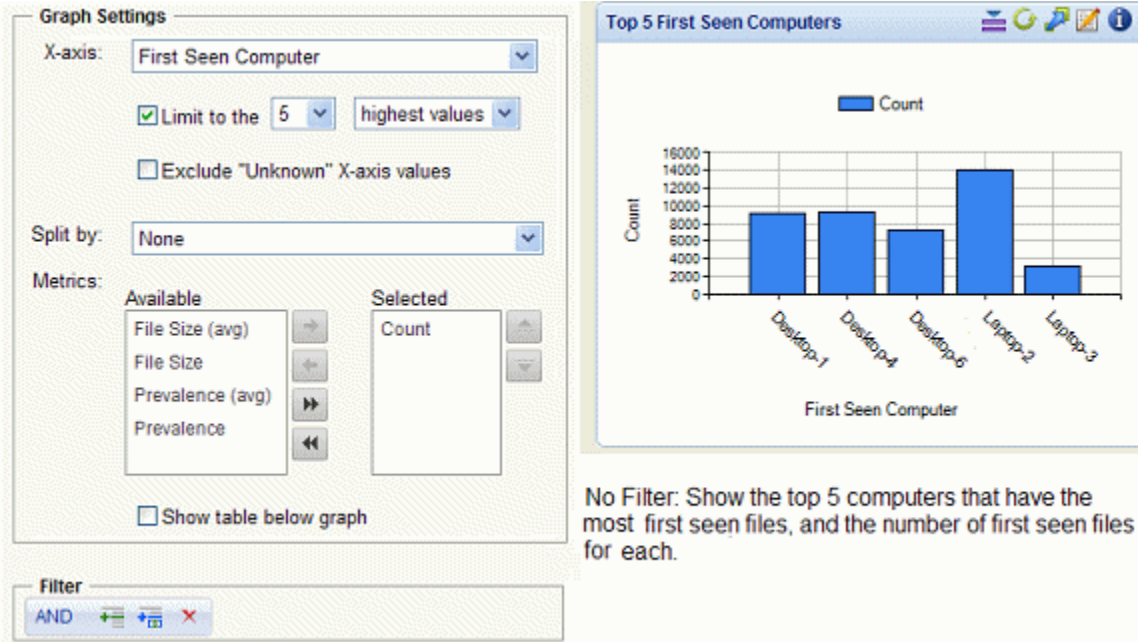
Every expression belongs to a group, even if the group includes only one expression. While an expression might evaluate to true on its own, the group operator determines whether the *group* is true, as [Table 94](#) shows.

**Table 94:** Group operators in portlet filters

Operator	Effect
<b>AND</b>	If <i>all</i> expressions in the group are <i>true</i> , the group is true. For the top-level group, this means that data for which all expressions in the group are true is displayed in the portlet.
<b>OR</b>	If <i>at least one</i> expression in the group is <i>true</i> , the group is true. For the top-level group, this means that data for which at least one expression in the group is true is displayed in the portlet.
<b>NOTAND</b>	If <i>at least one</i> expression in the group is <i>false</i> , the group is true. For the top-level group, this means that data for which at least one expression in the group is false is displayed in the portlet.
<b>NOTOR</b>	If <i>all</i> expressions in the group are <i>false</i> , the group is true. For the top-level group, this means that data for which all expressions in the group are false is displayed in the portlet.

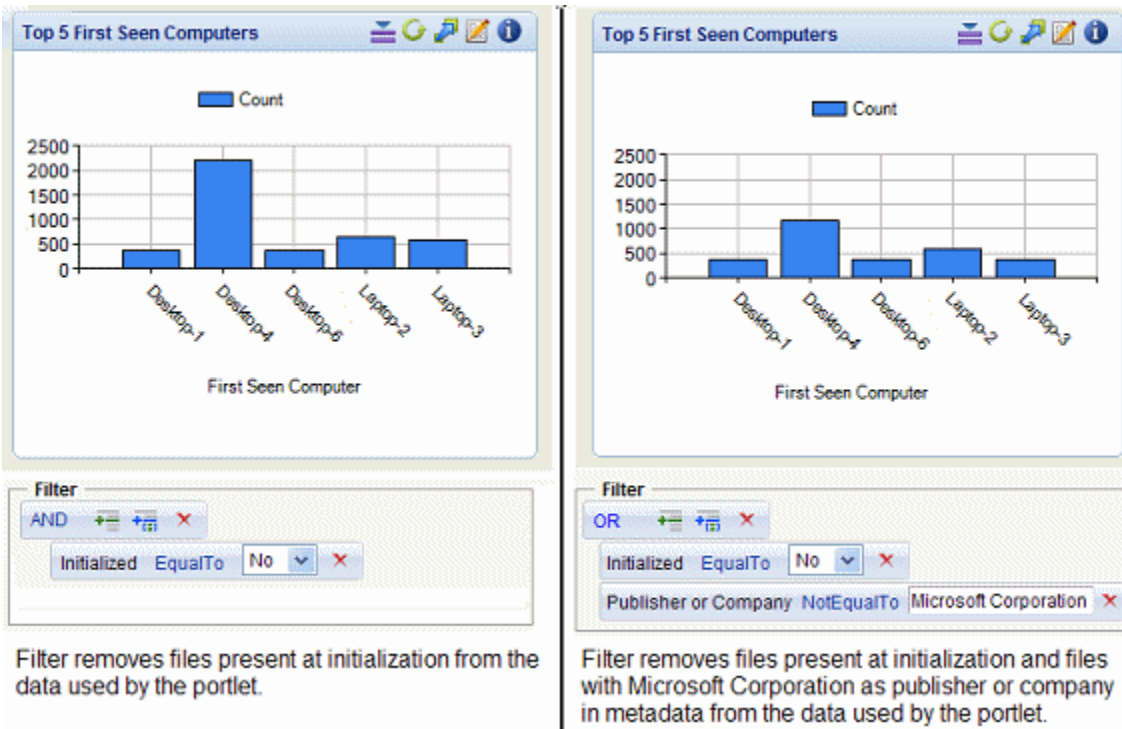
With **AND** as the group operator and a single expression, if the expression is true, the group is true, and the data matching the expression will be included in the portlet. As the table describes, however, adding expressions and using other operators can provide more powerful and complex filters. The illustrations below show some examples:





No Filter: Show the top 5 computers that have the most first seen files, and the number of first seen files for each.

If you created a “Top 5 First Seen Computers” portlet as shown in the details above, it displays the five computers that have the most first seen files. Note that there is not a filter on this data. Perhaps you would like to eliminate data for files that were on computers when the Bit9 Agent was installed and concentrate on anything that arrived afterward. To accomplish this, you could add an expression and create a filter to eliminate “initialized” files, as shown on the left, below.



Filter removes files present at initialization from the data used by the portlet.

Filter removes files present at initialization and files with Microsoft Corporation as publisher or company in metadata from the data used by the portlet.

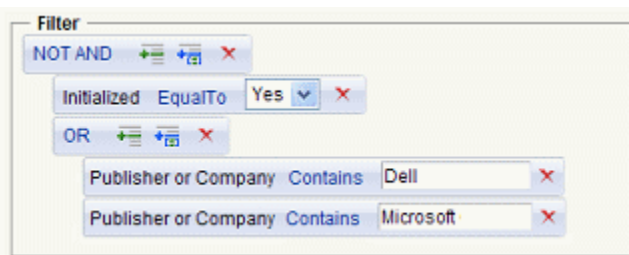
To further fine-tune your portlet, you might decide to eliminate all files that identify “Microsoft Corporation” as the publisher in addition to initialized files since you know that you installed several Microsoft applications on all computers after initialization and it is not necessary to track these in your portlet. To accomplish this, you could change the group operator to OR and create a new expression to produce a filter as shown in the right half of the illustration above.

As long as you can use the same group operator to accomplish your goal, you can continue adding expressions to a group.

## Nesting Groups of Expressions

You can nest groups of expressions within a filter. Each expression in a filter group shares the same top-level operator (i.e., AND, OR, NOT AND, NOT OR), and the results of the group are treated like an expression for the group above it. Group level can be determined by the indentation of the group and its expressions – those to the left are higher-level groups than those farther to the right.

The filter shown below indicates that files whose data is displayed in the portlet must NOT be both initialized AND either from Dell OR from Microsoft. The OR group is at the same level as the Initialized expression, and the NOT AND group contains everything in the filter.



### Note

Because some pre-processing of filters occurs as you choose each building block of an expression or group, you might notice a several second time delay after filter construction actions.

## Chapter 22

# Locating Files

This chapter explains how to use the Find Files page to locate or verify the existence of specific executable files on computers running the Bit9 Agent. Find Files locates *instances* of files, not their listings in the File Catalog.

### Sections

Topic	Page
<a href="#">Find Files Overview</a>	600
<a href="#">Initiating Find Files from Other Pages</a>	600
<a href="#">Defining a Search on the Find Files Page</a>	601
<a href="#">Using Find Files Results</a>	604
<a href="#">Saved Views for File Searches</a>	606

## Find Files Overview


The Bit9 Server keeps track of all “interesting” files on all connected computers running the Bit9 Agent, in near-real-time. Because of this “live inventory,” you can quickly locate a file or group of files matching a name, hash, or other criteria available in the database for your Bit9 Server. For offline computers, the file inventory includes all files from the last time they were connected.

This chapter focuses on the Find Files page, which opens by default with a filter that allows you to search for a file by name. As with the Files on Computers tab, you can add filters to fine-tune the results you get, and for many searches, you can create a Saved View. In addition, certain other console pages include a Find Files button or link that displays Find File results for a particular file described in a table row or details page.

### Notes

- You also can search for file instances on the Files on Computers tab of the Files page, although you will have to add all filters manually, including the file name filter.
- Certain features allow you to exclude files from the file inventory, and these may not appear in search results. See the Overview section of [Chapter 7, “File and Publisher Information,”](#) for details.

## Initiating Find Files from Other Pages

In addition to going directly to the Find Files page, you can search for file instances by clicking the Find File button  next to a file name or hash in some tables on other pages. This initiates a search by hash for all instances of that file. You can do this from:

- the Files page (both the Files Catalog tab and the Files on Computers tab)
- the File Group Details page
- the Baseline Drift Report Results page (Files views)
- the Snapshot Content page
- the Find Files page (to narrow results to instances of one specific file only)
- the Software Rules/Publishers page (to find all files from one publisher)
- the Approval Request Details page (to find all instances of the file whose approval is requested)

Certain other console pages have links that initiate a Find Files search pre-configured to find files relevant to the location you are in. These include:

- File name links on the Files page – When you click on a highlighted filename on the Files page, the console displays a Find Files report of all files *associated with* the named file (that is, files installed by or that are copies of the named file).
- File Details page and File Instance Details page – The *All File Instances* link in the Related Views menu initiates a search for the file whose details you are viewing.
- Add/Edit Policy page – The Related Views menu on this page has two file searches: *All Files on computers in this policy* and *Unapproved files on computers in this policy*.

- Computer Details page – The Related Views menu includes *Files on this Computer*, which displays a Find Files report of all files on the computer.

When Find Files results appear for any of these queries, you can further refine, as with any other console table, by showing or hiding columns and applying additional filters – if the Filters panel is not showing, click the Show/Hide Filters link.

Another tool for finding files appears on the Home Page dashboard, which includes a Find Files or Events portlet.

## Defining a Search on the Find Files Page

You can create file queries on the Find Files page based on any parameter available on the Filters menu. As with any page, you can combine filters, in some cases including more than one of the same type of filter (for example, *File Name is calc.exe* or *File Name is add.exe*) in the same search.

If you are searching for one specific file, you can search by file name or hash identifier.

### Tip

Combination searches based on file name and hash are useful for detecting attacks where a malicious program presents itself with different file names but contains the same data, which you can determine by comparison.

## Finding Files by Name

Although searching by hash is a better way to be certain you find all instances of a file, searching by name is the easiest type of search to create from scratch. File Name searches allow you to use different operators to expand or narrow the matches you get from the search, as shown in [Table 95](#).

**Table 95:** Operators for the File Name Filter

Field	Description
<b>contains</b>	Any file whose name <i>contains</i> the text in the box.
<b>does not contain</b>	Any file whose name does <i>not</i> contain the text in the box.
<b>begins with</b>	Any file whose name <i>begins with</i> the text in the box.
<b>ends with</b>	Any file whose name <i>ends with</i> the text in the box.
<b>is</b>	Only files that <i>exactly</i> match the text you enter. When you choose <b>is</b> , be sure to include the full file name, including extension, in the File Name text box.
<b>is not</b>	Any file whose name does not exactly match the text you enter. Note that if you enter “calc” as the File Name, for example, the results from <b>is not</b> <i>will</i> include “calc.exe”, “mycalc”, etc.
<b>is empty</b>	Any file whose name is missing or blank.
<b>is not empty</b>	Any file whose name is <i>not</i> missing or blank.

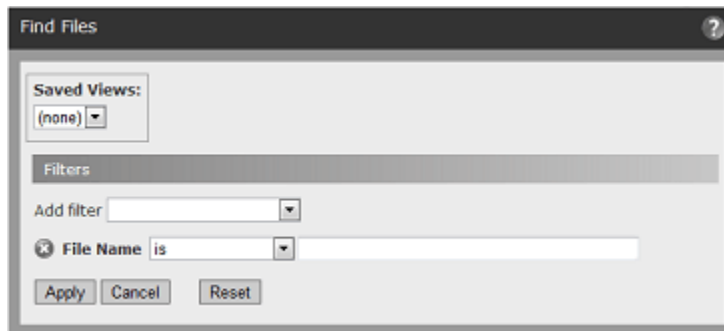
By default, the Find Files page opens with the File Name filter and the operator “is”, meaning file instances exactly matching the text you enter in the box will be in the results.

When searching for a file, consider the following best practices:

- **No Wildcards** – Do not use wildcards (\*, ?, etc.) in your search string for a file name. The Bit9 Server will attempt to match them literally, and the results will not likely be what you want. Instead, use the operator menu, which provides choices that accomplish the same thing, without requiring you to type in special symbols.
- **Case Sensitivity and Platforms** – Although case-sensitivity varies among operating systems, file searches in the Bit9 Platform are not case sensitive; for example, searching for “Myfile.exe”, myFiLE.exe”, or “myfile.exe” will return the same results
- **Limit Results** – Try to define your search parameters so that the results are limited to a reasonable number of files. The console does limit the number of matching files it will return, and you will see a message instructing you to try a narrower search if the number of results exceeds what can reliably be inserted into one table.
- **Auto-Completion** – Many fields on the Find Files page, including the File Name field, provide automatic matching of the string as you type it, showing matching choices in a menu.

**To locate instances of a file by name:**

1. In the console menu, choose **Tools > Find Files**. The Find Files page appears with the default filter, *File Name*, and the default operator, *is*.

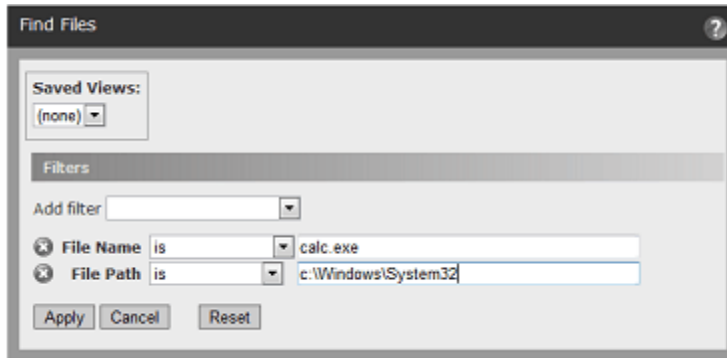


2. Specify a File Name, or a portion of a filename, that you would like to use in the search. As you type, console displays a list of files that match the string you have typed so far.
3. Choose an operator with which to match your file (see [Table 95](#)). For example, choose *contains* as the operator if you want to see any file that has the name you entered *anywhere* in its name. Choose *is* if you want only files exactly matching the File Name you entered.
4. Click **Apply**. All files (on all computers) matching the File Name-operator combination you entered are displayed in the Find Files table.
5. You can add other filters to the search if you choose, clicking **Apply** in the Filters panel each time you want to see new results.

## Adding a Pathname to a File Search

File Path is one possible addition to a search for files by name. It may also be useful in other searches, for example, if you want to find all files from a specific publisher in a specific directory and its subdirectories.

You specify a pathname *without* the name of the file you want to find. For example, if you wanted to find *calc.exe* in *c:\windows\system32*, you would specify the following filters:

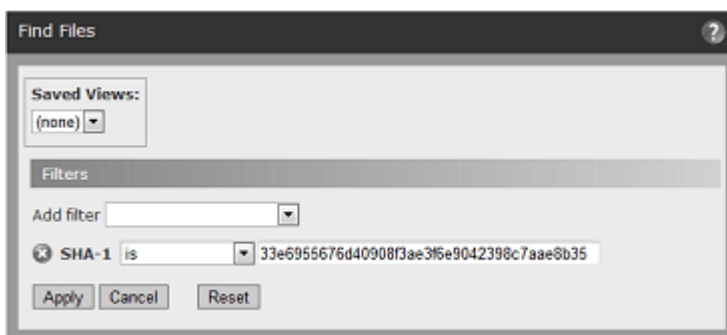


Specifying that the File Path **is** *c:\windows\system32* indicates that you want to find files only in the named folder, not in subfolders. If you want to search for all files in a named folder and its subfolders, you use the operator **contains**. For example, if you specified File Name is *calc.exe* and File Path **contains** *c:\windows\system32*, you would find all instances of *calc.exe* in *system32* and at any level underneath it.

**Platform Note:** Keep in mind that using a pathname in a file search will limit your search to computers that match the platform-specific delimiters (i.e., ‘\’ or ‘/’) and other special path characters you use.

## Finding Files by Hash

Bit9 supports three hash types: SHA-256, SHA-1, and MD5. If you have a hash from some source other than Bit9 and want to search for it, you can search for that file on your computers from the Find Files page by choosing the hash type from the Filters menu entering the hash into the filter field.





On some files, Bit9 does special processing to create SHA-256 hashes that will be identical for identical files. Because of this, use of externally created SHA-256 files is not recommended.

The best way to search by hash is to locate the file of interest in one of the Files tabs and then click on the Find File button next to the file. The console will run the Find File search without you needing to type or cut and paste the hash string.

As with file names, the console shows a list of matching hashes as you type in digits, and if there is only one item on the list, you can pick it without entering the entire hash string.

## Using Find Files Results

The Find Files results page provides all of the tools available on the Files page, both for getting further information and taking action on one or more files in the table:

- When your initial search is broad enough to include different files (not just different instances) in the results, you can initiate a new search for all instances of one specific file by clicking the Find File button  next to that file.
- You can click the View Details button  next to any found instance of the file to get more information about that instance.
- You can select files from the results and operate on them with the approval or ban commands on the Action menu. For example, you can **Approve Locally** or **Remove Local Approval** for any file in the results by checking the box to the left of the file listing and clicking the appropriate button.
- If you have Bit9 Software Reputation Service (SRS) enabled, you can view additional information (if available) for any file in the results by checking the box to the left of the file name and choosing **View Bit9 SRS Cloud Data** from the Action menu.
- If you have enabled third-party analysis tool integrations via the Bit9 Connector, **Analyze with ...** commands appear on the Action menu. You can use the available commands to send one or more of the found files for analysis.
- The Action menu also includes commands that allow you to find computers that have, or are missing, one or more files in the Find Files results.

### Notes

- Each file for which you use the View Bit9 SRS Cloud Data command opens the results in its own tab. For multi-file requests in Internet Explorer, the popup blocker may block the results for each file after the first one.
- As in other console tables, buttons in the table head for Find Files results enable you to rearrange display columns, download results in comma-separated-value format, and add the Find File results to a Snapshot. For more information, see [Bit9 Console Tables](#) in [Chapter 2, “Using the Bit9 Console.”](#)

## Special Cases in Results

### Files on Offline Computers

If a computer is offline, a Find Files search will include the matching files from that computer’s most recent synchronization with the Bit9 Server in the results. The next time the computer connects to the Bit9 Server, its file information is updated within a short time



(depending upon the network traffic and how many computers are being updated), and the updated information becomes available to Find File.

Find File results tables that include the Computer column have an indicator to the left of the computer name showing whether the computer is connected and up-to-date. A darker blue circle indicates that the computer is connected and up-to-date. An orange circle indicates a computer awaiting upgrade. A light blue circle indicates a disconnected computer. When you move the mouse cursor over a status circle, more information for that computer's status appears below the name, including how long a computer has been offline.

	Date Created v	Computer	File Name	Trust	Threat
	Oct 07 2011 05:20:34PM	MYCORP\DESKTOP-3	sol.exe	9	
	Oct 07 2011 05:15:47PM	MYCORP\DESKTOP-4	sol.exe (Deleted)	9	
	Sep 28 2011 05:08:47PM	MYCORP\LAPTOP-5 Disconnected for 17 day(s)	sol.exe	9	
	Sep 28 2011 05:07:18PM		sol.exe	9	

## Files on Deleted Computers

If a computer has been deleted from the Computers list, its files remain in the database of Files on Computers for one day. This means that a Find Files search could include results from deleted computers. Deleted computers are labeled as such in the Find Files results.

	Date Created v	Computer	File Name	Trust	Threat
	Oct 07 2011 05:20:34PM	MYCORP\DESKTOP-3	sol.exe	9	
	Oct 07 2011 05:15:47PM	MYCORP\DESKTOP-4	sol.exe	9	
	Sep 28 2011 05:08:47PM	MYCORP\LAPTOP-5	sol.exe	9	
	Sep 28 2011 05:07:18PM	MYCORP\LAPTOP-2	sol.exe	9	
	Jul 18 2011 05:16:42PM	MYCORP\DESKTOP-7 (Deleted)	sol.exe	9	

## Deleted Files

If a file matching a Find Files search has been recently deleted from a computer, it can be included in Find File results if you choose, although this is not done by default. To include deleted files, check the *Show deleted files* box in the bottom right of the Find Files page; the table is immediately updated to show any deleted files matching your search parameters. Deleted files are labeled as such in the Find Files results.

	Date Created v	Computer	File Name	Trust	Threat
	Oct 07 2011 05:20:34PM	MYCORP\DESKTOP-3	sol.exe	9	
	Oct 07 2011 05:15:47PM	MYCORP\DESKTOP-4	sol.exe (Deleted)	9	
	Sep 28 2011 05:08:47PM	MYCORP\LAPTOP-5	sol.exe	9	
	Sep 28 2011 05:07:18PM	MYCORP\LAPTOP-2	sol.exe	9	

Deleted files are removed from the database on the same schedule as old events. See [“Advanced Configuration Options”](#) on page 627 for information about configuring this time period.

#### Notes

- If you are searching for deleted files using the Deleted filter, you must check the *Show deleted files* box in the bottom, right corner of the page before any matching results will appear.
- Including deleted files in a search will slow down the search and consume more resources, so use this feature only when necessary.

## Files on Computers Still Initializing or Synchronizing

If a computer has just had the Bit9 Agent installed and is still initializing, some of its files are available to Find Files, but its full file inventory is not available until initialization is complete. To determine whether a computer is still initializing, go to the Computers page and search for the computer.

Similarly, if an agent is re-synchronizing with the server, changes in its file information are not complete until the synchronization is finished. You can view synchronization progress on the Computer Details page or, if you add the Synchronization column to the table, on the Computers page.

## Saved Views for File Searches

If you have a complex search that you think you will use often, you may be able to save it as a Saved View.

#### Notes

- Certain Find File reports, including those initiated from the Find File button on other pages, cannot be saved because they were run in a specific context that might not be in effect if executed again from the Find Files page – the Saved Views panel does not appear in these cases. As an alternative, you might be able to duplicate and save the search you want by using filters on the Files on Computers tab of the Files page.
- ReadOnly users cannot save views. Also, some custom login account groups might not have permission to save views.

#### To create a Saved View on the Find Files page:

1. In the console menu, choose **Tools > Find Files**. The Find Files page appears with the default filter, *File Name*, and the default operator, *is*.
2. Choose each filter you would like to add to the search criteria, provide any text required to configure the filter, and click **Apply**.

3. When you have finished adding filters, enter a name in the Saved Views box above the table and then click **Add**. You now will be able to choose the Saved View you created from the Saved Views menu and get results for this same search whenever you choose.



## Chapter 23

# System Configuration

This chapter explains settings that enable you to configure and maintain your Bit9 Server installation. Access to the System Configuration page is available only to login accounts in the Administrators group or in customized groups with View System Configuration and Manage System Configuration boxes checked.

**Sections**

Topic	Page
<a href="#">Overview</a>	610
<a href="#">Viewing Server Status and Options</a>	612
<a href="#">Configuring Active Directory Integration</a>	614
<a href="#">Configuring Agent Management Privileges</a>	615
<a href="#">Managing the Bit9 Event Database</a>	618
<a href="#">Securing Agent-Server Communications</a>	623
<a href="#">Advanced Configuration Options</a>	627
<a href="#">Backing Up the Bit9 Server</a>	631
<a href="#">Restoring the Bit9 Server</a>	634
<a href="#">Configuring Alert and Approval Request Mail</a>	635
<a href="#">Managing Bit9 Platform Licenses</a>	640
<a href="#">Activating Bit9 SRS</a>	643
<a href="#">Activating Carbon Black Server Integration</a>	648

## Overview

The System Configuration pages present both read-only status information and configurable settings for use by Bit9 Security Platform Administrators. The configuration information is organized on a series of tabbed views, some of which have several panels:

- **General** tab – Server status information, options for integrating Bit9 with Active Directory or LDAP, and Bit9 Agent Management options.
- **Events** tab – Configuration settings for managing Bit9’s own database and options for setting up supplemental external event logging, including Syslog.
- **Security** tab – Shows current status of secure communications between Bit9 Agents and the Bit9 Server, and provides options for enabling certificate verification for these communications if not already enabled.
- **Advanced Options** tab – Options for database backup, automatic agent upgrades, Bit9 Console login timeout, files for Bit9 to ignore, Bit9 API access, deleting offline computers, allowing use of expired publisher certificates, and letting Bit9 Software Reputation Service (SRS) update detection indicators, system health indicators, and definitions of updaters.
- **Mail** tab – Configuration settings for sending email when a Bit9 alert is triggered or an approval request is resolved.
- **Licensing** tab – Shows the number and type of Bit9 Agent licensed for your server, and allows you to update your license key; also allows you to enable and configure Bit9 Software Reputation Service.
- **Connectors** tab – Configuration settings for integrating the Bit9 Server with one or more network security devices or services. See [Appendix C, “Bit9 Connector for Network Security Devices,”](#) for information about the settings on this tab.
- **External Analytics** tab – Configuration settings for Bit9 External Analytics, which enables the Bit9 Server to export data it collects from endpoints to external analysis tools. See [Appendix F, “Exporting Bit9 Data for External Analysis,”](#) for information about the settings on this tab.

### To display the System Configuration page:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. By default, the Bit9 Console displays the General tab of the System Configuration page. Select another tab if you want to view or change something not on this tab.

## The General Configuration Tab

The General tab of the System Configuration page has three sets of configuration fields:

- The [Server Status](#) panel shows information about your Bit9 and database servers, including their addresses.
- The [Active Directory/LDAP Integration](#) panel allows you to configure AD or LDAP integration with the Bit9 Server.
- The [Agent Management](#) panel allows you to set up access to special agent management commands by user, group, or password.

The screenshot shows the 'System Configuration' window with the 'General' tab selected. The window is divided into three main sections:

- General Settings** (Server Status):
  - Bit9 Security Platform Version: 7.2.0.133 P0
  - Server Address: Server2.mycorp.local
  - Server Port: 41002
  - Server Timezone: -Automatic-
  - Database Schema Version: 7.2.0.133
  - Database Address: local
  - Database Auth.type: NT
  - Database Size: 263.19 MB
  - Free Local Disk Space: 24.7 GB / 40.0 GB
  - CL Version: 920
- Active Directory / LDAP Integration**:
  - AD-Based Logins: Disabled
  - AD Security Domain: (empty text field)
  - AD-Based Policy: Disabled
  - Windows 2000 DCs:
  - Test AD Connectivity:
- Agent Management**:
  - Windows User/Group To Manage Agents:  None  User or group  Pre-defined group
  - Mac User/Group To Manage Agents:  None  User  Group
  - Linux User/Group To Manage Agents:  None  User  Group
  - Enable Global Password:
  - Enter Password: (password field)
  - Confirm Password: (password field)

At the bottom of the window are three buttons: Edit, Update, and Cancel.

## Viewing Server Status and Options

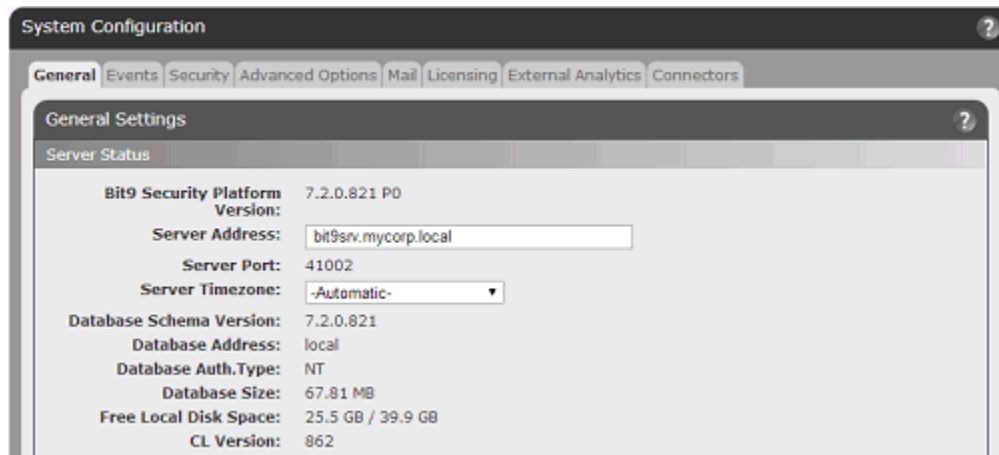
The top panel on the General tab of the System Configuration page is *Server Status*, which displays Bit9 Server parameters and allows editing of some of them (see [Table 96](#) for details).

### Important

Parameters on the Server Status panel tell you about the size of the Bit9 database and the amount of free space on the computer running Bit9 Server. These do not, however, report on whether an *external* SQL database is running out of space. Regardless of which database option you choose, you should monitor your Bit9 database regularly to be sure it does not overflow and prevent the Bit9 Server from operating. See the *Installing Bit9 Server* manual for more information on database configuration. Also, see “[Creating Alerts](#)” on page 498 for information on database-related alerts.

### To display server status information:

1. On the console menu, choose **Administration > System Configuration**.
2. If it is not already showing, click on the **General** tab. The General configuration options appear, with the Server Status panel showing at the top.



3. To change timezone, click the **Edit** button, make the changes, and click **Update**, and then click **Yes** on the confirmation dialog. See [Table 96](#) for details about the other settings.



**Table 96:** Server Status Information and Configuration Options

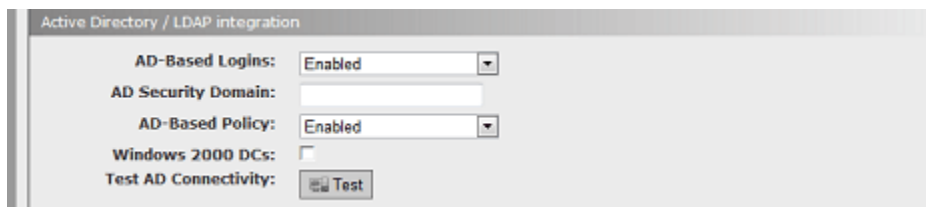
Field	Description
<b>Bit9 Version</b>	Version number of the installed Bit9 Server software. (Read Only)
<b>Server Address</b>	<p>IP address or qualified DNS name for the Bit9 Server.</p> <p>If you change the server address, you must reinstall the Bit9 Agent on all computers (although not if you change from an IP address to an equivalent DNS name, or vice versa). As soon as the agent is installed, computers reinitialize and all files except those explicitly banned on the server become locally approved and permitted to run. So that you can use the same policies, the Bit9 Security Platform automatically updates existing agent installation packages with the new IP address so that they direct computers to report to the correct server when they come back online.</p> <p><b>Note:</b> IPv6 may be used for communications with the Bit9 Server, but a numeric IPv6 address may not be accepted in certain versions of the Firefox browser. To avoid this problem, use one of the other supported browsers or a fully qualified DNS name.</p>
<b>Server Port</b>	Bit9 Server port that is dedicated to communications with computers running the Bit9 Agent. This cannot be changed after server installation. (Read Only)
<b>Server Timezone</b>	The timezone used by the Bit9 Server. Normally this will be set to Automatic, which uses the same time zone as the operating system on the Bit9 Server. However, to account for non-standard handling of daylight saving time in certain zones, you can set the server timezone explicitly, using the dropdown menu here.
<b>Database Schema Version</b>	Normally the database schema version is the same as the Bit9 Server version. You can, however, use existing databases when you upgrade or reinstall the server. In this case the database schema version can be different. For Bit9 Support use. (Read Only)
<b>Database Address</b>	Shows whether your database is <b>Local</b> or on a separate server, in which case it provides the address. (Read Only)
<b>Database Auth. Type</b>	This indicates the type of database authorization you chose when you installed Bit9 Server. It is either <b>NT</b> , indicating that you are controlling database access by Windows NT account or group, or <b>SQL</b> , indicating that you are using a login and password specific to your SQL Server. (Read Only)
<b>Database Size</b>	Amount of disk space currently used by the Bit9 database. (Read Only)
<b>Free Local Disk Space</b>	<p>Amount of available <i>local</i> disk space on the Bit9 Server. If the Bit9 database is on the same system as the Bit9 Server, you can periodically monitor this value to determine how quickly events are accumulating and whether you need to adjust the event log deletion period. (Read Only)</p> <p><b>Important:</b> This field reports free space on the Bit9 Server system only. If you are using a remote database, you must check available space directly on that system.</p>
<b>CL Version</b>	This is a configuration list version number reflecting the current set of policy rules. As Bit9 Console users create bans, changes policies, and take other actions that change the configuration of your Bit9 Server, this number increments. Bit9 Support can use CL version in certain troubleshooting situations. (Read Only)

## Configuring Active Directory Integration

Bit9 Server can take advantage of your Active Directory (AD) environment to set access privileges for users of the Bit9 Console, assign security policies to computers, provide user and computer metadata, and designate certain groups or users to be able to install software (and have it automatically approved) on Bit9-managed computers. You configure AD integration on the General tab.

### To display AD integration configuration options:

1. On the console menu, choose **Administration > System Configuration**.
2. If it is not already showing, click on the **General** tab. The General configuration options appear, with the AD/LDAP integration options showing in the middle panel.



3. To configure AD or LDAP integration, click the **Edit** button at the bottom of the page, make the needed changes in the Active Directory/LDAP integration panel, click the **Update** button, and then click **Yes** on the confirmation dialog. See [Table 97](#) for details about these settings.

**Table 97:** Active Directory/LDAP Integration Options

Field	Description
<b>AD-based logins</b>	Choosing <b>Enabled</b> in this field allows users to log in to the Bit9 Console using AD accounts and passwords. See <a href="#">“Enabling Console Access via AD Accounts”</a> on page 77 of <a href="#">Chapter 3, “Managing Console Login Accounts,”</a> for more detail.
<b>AD security domain</b>	Specifying an AD security domain in this field directs the Bit9 Server to look in that domain for the Bit9 security groups for Bit9 Console user login validation. If you do not specify a security domain, the login domain for each console user is used, and so the Bit9 security groups must be in each user’s domain for that user to be able to log in.
<b>AD-based policy</b>	Choosing <b>Enabled</b> in this field allows you to automatically assign Bit9 policies to computers based on AD or LDAP. See <a href="#">Chapter 4, “Managing Computers,”</a> for more detail.
<b>Windows 2000 DCs</b>	Checking this box indicates that your network is using Windows 2000 domain controllers. This disables the AD security domain value you provided, if any, since it relies on cross-domain membership tests that are only available with Windows 2003 SP2 domain controllers.
<b>Test AD Connectivity</b>	Clicking the <b>Test</b> button tests connectivity between the Bit9 Server and Active Directory. If it reports Success, you should be able to use Bit9’s Active Directory integration features. If it reports Error, your Bit9 Server cannot access Active Directory, and you will need to resolve this problem before the integration features can be used.

## Configuring Agent Management Privileges

You may, in conjunction with your Bit9 Technical Support representative, use special Agent Management commands for Bit9 Agent management. Each agent has its own unique command-enabling “CLI” password, which you can look up in the Bit9 Agent tab of the Computer Details page. You might, however, want to create a global access method so you don’t have to look up the password for each agent.

Because Bit9 Agent plays a critical role in managing and protecting your computers, you can and should limit access to these commands. In the Agent Management section of the General tab, you can choose one or both of the following methods for controlling agent command access:

- for each client platform, you can specify a user or group allowed to run the commands
- you can specify a password that will be required to run the commands

If you define both a user/group and a password, *either* access method is sufficient on its own. The current agent management configuration when agent installation packages are created is built into the agent. If you change the password, the Bit9 Server updates online agents with the new password, but agents not online must continue using the old password. Likewise, changes in the user or group access definition are not effective on an offline agent unless the old agent is uninstalled and a new one is installed by some method.

### Note

Configuring the Agent Management options *before* generating any agent installation packages is the most efficient way to set a global agent password or user/group access choice.

For new installations of Bit9 Server, you are prompted to provide an Agent Management access method during the installation process – this is the best time to choose an option.

### To display agent management configuration options:

1. On the console menu, choose **Administration > System Configuration**.
2. If it is not already showing, click on the **General** tab. The General configuration options appear, with the Agent Management options showing in the bottom panel.

The screenshot shows the 'Agent Management' configuration interface. It includes the following elements:

- Windows User/Group To Manage Agents:** Radio buttons for  None,  User or group, and  Pre-defined group.
- Mac User/Group To Manage Agents:** Radio buttons for  None,  User, and  Group.
- Linux User/Group To Manage Agents:** Radio buttons for  None,  User, and  Group.
- Enable Global Password:** A checked checkbox.
- Enter Password:** A text input field with masked characters (dots).
- Confirm Password:** A text input field with masked characters (dots).

- To configure agent management, click the **Edit** button at the bottom of the page, make the needed changes, click the **Update** button, and then click **Yes** on the confirmation dialog. See [Table 98](#) and “[Connection Status and Agent Management Choices](#)” on page 616 for more details about these settings and guidance on choosing options.

**Table 98:** Agent Management Configuration Options

Field	Description
<b>Windows User/ Group to Manage Agents</b>	<p>If defined, the specified Windows user or group is allowed to run special commands for Bit9 Agent management on computers that recognize that user or group.</p> <ul style="list-style-type: none"> <li>Choose the <i>User or group</i> radio button to enter a user or group name manually; you also can enter a user or group SID in this box.</li> <li>Choose the <i>Predefined group</i> button to choose a Windows group (e.g., Local Administrators), from a menu.</li> </ul>
<b>Mac User/ Group to Manage Agents</b>	<p>If defined, the specified Mac user or group is allowed to run special commands for Bit9 Agent management on computers that recognize the user or group. Choose the <i>User</i> radio button or the <i>Group</i> button and enter a name in the box.</p>
<b>Linux User/ Group to Manage Agents</b>	<p>If defined, the specified Linux user or group is allowed to run special commands for Bit9 Agent management on computers that recognize the user or group. Choose the <i>User</i> radio button or the <i>Group</i> button and enter a name in the box.</p>
<b>Enable Global Password</b>	<p>If defined, the specified password may be used by <i>any</i> user to run special commands for Bit9 Agent management from the client computer. Check the box to enter the password.</p> <p>If you define both a password and a user or group for agent management, you only need one or the other for access.</p>

## Connection Status and Agent Management Choices

Your Agent Management access choice may be dictated by whether or how often your client systems running the Bit9 Agent are connected to the Bit9 Server.

If a computer is *never connected to the server*, you can provide access by choosing an Agent Management password before generating installation packages. This password is built into the agent, and can be changed only by one of the following means:

- installing a new agent package generated after the password change
- importing a new configuration list from Bit9 Server after you have changed the global password; see your Bit9 Technical Support representative for instructions on importing a configuration list

Another option for systems never connected to Bit9 Server is specification of a group that can be guaranteed to exist on all machines, such as Local Administrators for Windows computers. The suitability of this method depends on how your organization manages administrative accounts, but it lets you control access to agent management commands by adding or removing users from the named group, independent of changes in the Bit9 Security Platform.

If a computer will be *connected to Bit9 Server occasionally*, you have more flexibility in choosing and changing client management access methods. Changes to a password, or to user or group definition, propagate to the agents the next time they connect.

If all of your computers will *always be connected to Bit9 Server* (or can be if needed), you have the most flexibility in configuring Agent Management access since changes you make will go to your connected agents as soon as the agent and server are in contact. In this case, you might find it more convenient to choose a well-known group, or define a new group, such as "Bit9 Local Administrators", and give its members access to the management commands. Groups also allow the use of such tools as *runas*, *psexec*, or *sudo*, to run commands using alternate credentials. You also can use a password if you choose.

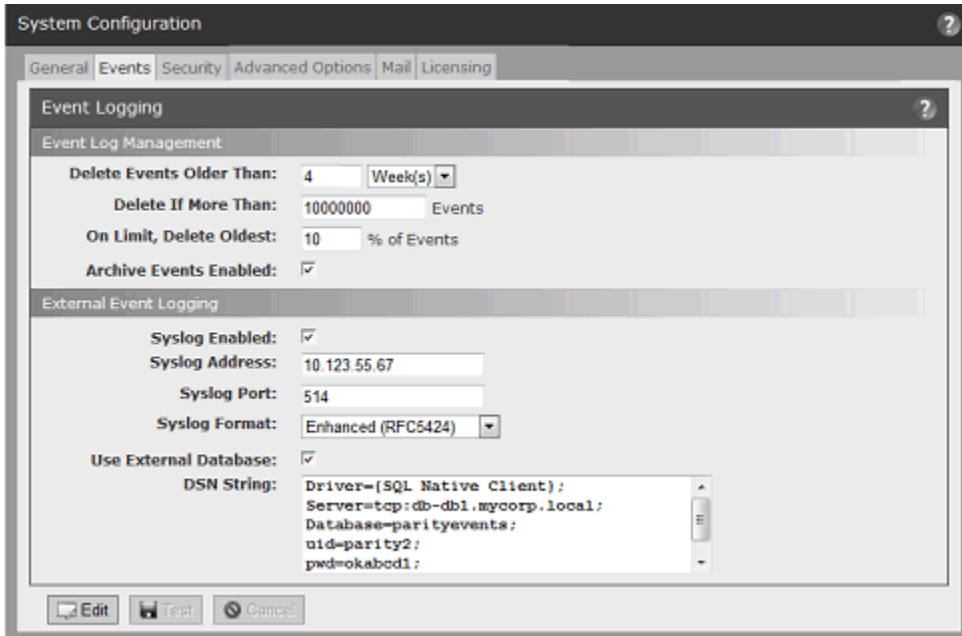
**Note**

When running on Windows Vista and later, membership in pre-defined security groups like Administrators requires that the application run as an administrator. If you are not certain that a user has this elevated privilege, using a built-in group for Agent Management access may not be a good choice if you will be using computers running Vista or Windows 7.

## Event Management Options

Bit9 event data is stored in a SQL Server database, and grows over time at a rate that corresponds to file activity on your network. The Events tab provides two sets of options for managing events data generated by the Bit9 Security Platform:

- The Event Log Management panel provides options for managing the size of the *primary* Bit9 database and for archiving events.
- The External Event Logging panel provides options for enabling supplemental, external logging of Bit9 events to another SQL Server or a Syslog management server. Use of supplemental external logging may allow you to reduce the amount of data you keep in the primary database.



### Important

Your choices for event log management may be determined by your disk capacity and the availability of an external SQL Server database for storing Bit9 data. Please consider this before making any changes to your logging configuration.

## Managing the Bit9 Event Database

The Event Log Management tab includes options for limiting the growth of the Bit9 database and setting up event archiving.


### Setting Limits for Event Deletion

You can set limits that delete data to keep the Bit9 database at a reasonable size. Bit9 Server provides several mechanisms for handling this volume of data. Bit9 provides for automatic deletion of event data based on two different parameters:

- **Delete Events Older Than** – By default, Bit9 automatically deletes events older than 4 weeks, which means that event data is purged on the system and is not available for display in reports generated by the Bit9 Server. You can modify the time period in the Management Configuration table.
- **Delete if More Than** – This threshold defaults to 1 million for SQL Server Express and 10 million for other SQL Server editions. This works with a second parameter, **On Limit Delete Oldest**, which allows you to define the percentage of the events deleted when you reach the limit you set. The default percentage is 10%.

Event data is deleted when *either* condition is met. You can configure these automatic deletion parameters based the available disk space on the SQL Server and your need for historical information. To determine the right values for your network, monitor disk space use on the server and adjust the event database deletion parameters accordingly.

## Enabling Daily Event Archiving

If *Archive Events Enabled* is checked on the System Configuration Events tab, Bit9 Server generates a separate compressed CSV file for each day's event data. Daily event files are stored for one year and accessible through the Event Log Archives, which lists the date-stamped files in chronological order. Through the log, you can click on and open (or save to another location) any listed event log file. You open the Event Log Archives by clicking the Archives button  in the header of an Event log.

If *Archive Events Enabled* is not checked, no event archives are generated from that point forward.

## Moving the Database to an External Server

When you installed the Bit9 Server, one of your choices was whether to put the Bit9 database on the same computer as the Bit9 Server. You might find that the volume of Bit9 data requires a transition from a shared to a dedicated database server.

Moving the primary Bit9 database requires steps outside of the Bit9 Console, including running the Bit9 Server installation program to reconnect to the new server. Contact Bit9 Technical Support if you need to make this transition.

### Note

The External Event Logging options on the System Configuration Events tab are for enabling *supplemental* event logging, not for moving the primary database.

## Setting up External Event Logging

The Bit9 Security Platform allows you to copy event data to an additional, external SQL Server. You also can configure event output to a Syslog server using several different output formats. The full set of settings for external event logging are shown in [Table 99](#) on page [622](#).

## Logging Events to a Syslog Server

Bit9 Server supports integration of its event information with Syslog servers using several formats. You configure Syslog integration in the External Event Logging panel of the Events tab.

The supported formats are:

- **Basic (RFC3164)** – the default for upgrades to v7.2.1 from pre-6.0.1 Bit9 (Parity) versions
- **Enhanced (RFC5424)** – a newer standard and the default for new installations of Bit9 (Parity) v6.0.1 and later.
- **CEF (ArcSight)** – the format to use to integrate Bit9 event logs with HP ArcSight ESM or HP ArcSight Logger



- **LEEF (Q1 Labs)** – the format to use to integrate Bit9 event logs with QRadar Log Manager or QRadar SIEM

### Notes

- See the separate document *Bit9 Events Integration Guide* for more information on syslog formats supported by Bit9 and how to map Bit9 events to them.
- If you used HP ArcSight or Q1Labs products with previous Bit9 versions, you will need to see the Integration guide for information about upgrading your integration to Bit9 Security Platform v7.2.1.
- If you worked with Bit9 Technical Support to manually enable special Syslog formatting in pre-6.0.2 releases, your changes will be overwritten on upgrade to v7.2.1. Use the Syslog format menu to choose formatting.

### To enable event logging to a Syslog server:

1. Prepare the Syslog server to which you want to log Bit9 events. See the separate *Bit9 Events Integration Guide* for more details about preparing the server.
2. On the Bit9 Console menu, choose **Administration > System Configuration**, and on the System Configuration page, click on the **Events** tab.
3. On the Events tab, click the **Edit** button at the bottom of the page.
4. In the External Event Logging panel, check the **Syslog Enabled** box.



External Event Logging

Syslog Enabled:

Syslog Address: 10.123.55.67

Syslog Port: 514

Syslog Format: Enhanced (RFC5424)

5. Provide the address (IP address or FQDN) and port number of your Syslog server in the Syslog Address and Syslog Port boxes, respectively.
6. Choose the output format from the Syslog Format menu.
7. Click **Update** and choose **Yes** on the confirmation dialog to save your configuration.

### Logging Events to a Supplemental SQL Server

External logging gives you the option of creating custom report implementations directly through SQL. Using an external server can also allow you to meet forensic or compliance requirements for long-term event storage while maintaining events for a shorter period in the Bit9 Server database. You might also choose to implement external event logging for performance reasons.

Note several key points about what happens when external logging is activated:

- External logging does not eliminate local logging in the primary SQL Server database. Event logging continues, and saves events for whatever time period (or total number of events) you specify.



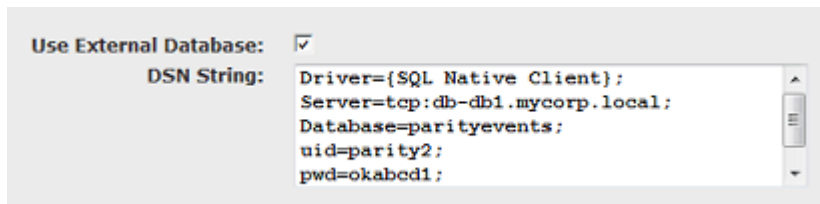
- To facilitate better system performance, event data is copied from the primary SQL Server database to the external event SQL Server database approximately every 30 seconds rather than continuously.
- Events that happened prior to your activation of external logging are not copied to the external log, so if you intend to set up external logging and want it to be comprehensive, it is best to do so at the same time you are setting up Bit9 Server.
- If the external server becomes inaccessible, an error is logged, but there will be no change in Bit9 Server behavior. Once the external server is available again, events that were missed will be copied.

Table 99, “External Event Logging Options,” on page 622 describes each of the parameters on the External Event Logging panel of the Events tab. See the Bit9 Support website or contact Bit9 Support for additional details.

The following describes the high-level procedure for setting up external event logging to a supplemental SQL database. If you want to use NT Authentication for your external database, use the special DSN shown in the following procedure.

**To enable external event logging to an additional SQL server:**

1. Install SQL Server on a machine with sufficient capacity for Bit9 event logging. Be sure to note the information for the DSN (Data Source Name) string – this will be necessary for use in the Bit9 Console.
2. Run the external-events script **external\_events.sql** to configure the SQL database so that it can properly store Bit9 events. This script is located in the **Bit9 Server\sql** folder. It must be run on the newly installed SQL Server before you can use external events logging.
3. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
4. Click on the **Events** tab. The External Event Logging panel appears.
5. Click the **Edit** button and then check the *Use External Database* box. This activates the **Test** button as well as the data fields on the panel.
6. In the DSN String field, enter the DSN for this database.
  - a. For manual authentication, this will include the following, each on its own line and separated by semicolons (the illustration following shows an example):
    - Driver={SQL Native Client};
    - Server=**tcp:yourfullyqualifiedservername\instancename**;
    - Database=**bit9Events**;
    - Uid=*usernameforSQLadmin*;
    - Pwd=*password*;



- b. You can use NT authentication, using the Domain credentials you supplied during Bit9 Server installation, for access to the external event logging server. To do this, replace the “Uid” and “Pwd” lines shown above with a “Trusted\_Connection” line in the following format:
- Driver={SQL Native Client};
  - Server=**tcp**:*yourfullyqualifiedservername\instancename*;
  - Database=**bit9Events**;
  - Trusted\_Connection=**Yes**;

**Note**

If you have difficulties with the DSN string, see the file **shepherd.dsn** in the Bit9 Server home directory.

7. To make sure your DSN works, click the **Test** button. If your DSN was configured appropriately, a “Testing: Success” message appears below the DSN String box. Otherwise, you will see an error message.
8. Once your DSN Test has succeeded, click the **Update** button (this replaces the “Test” button when the test is successful and you check the checkbox) and choose **Yes** on the confirmation dialog. This activates external logging.

**To disable external event logging:**

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click on the **Events** tab. The External Event Logging panel appears.
3. Click the **Edit** button. This activates the data fields on the panel.
4. Click the **Use External Database** box to remove the check. This turns the “Test” button into an “Update” button.
5. Click **Update** and choose **Yes** on the confirmation dialog. External event logging is disabled.

**Table 99:** External Event Logging Options

Field	Description
<b>Syslog Enabled</b>	A checkbox determining whether Bit9 event information is output to another server for further analysis with a Syslog management tool. If checked, you also must specify a Syslog server address and listening port. This option is off by default. <b>Note:</b> Contact Bit9 Technical Support for guidance on using Bit9 event output with your Syslog management tools.
<b>Syslog Address</b>	IP address for a Syslog server (optional). If you specify a Syslog address, you must also enter a port for the server. <b>Note:</b> No error is reported if you set the Syslog address and/or port incorrectly. To verify that Syslog address is correctly set, confirm the receipt of Bit9 events on the Syslog server after you have completed this configuration.

Field	Description
<b>Syslog Port</b>	<p>Port number for a Syslog server.</p> <p>Bit9 events directed to the listening port include activity messages such as blocked files, new files on the system, and changes to login accounts.</p> <p>If you export event data, events continue to be written to the Events page, which is accessible from the Bit9 Console. If you specify a Syslog port, you must also enter an address for the Syslog server.</p>
<b>Syslog Format</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• <b>Basic (RFC3164)</b> – this is the default for upgrades from pre-6.0.2 Bit9 versions</li> <li>• <b>Enhanced (RFC5424)</b> – this is a newer standard and the default for new installations beginning in Bit9 v7.0.1.</li> <li>• <b>CEF (ArcSight)</b> – format to use if you want to integrate Bit9 event logs with HP ArcSight ESM or HP ArcSight Logger</li> <li>• <b>LEEF (Q1Labs)</b> – format to use if you want to integrate Bit9 event logs with QRadar SIEM or QRadar Log Manager</li> </ul> <p>See the separate document <i>Bit9 Events Integration Guide</i> for more information on syslog formats supported by the Bit9 Security Platform and how to map Bit9 events to them.</p> <p><b>Note:</b> If you worked with Bit9 Technical Support to manually enable special Syslog formatting in pre-6.0.2 releases, your changes will be overwritten on upgrade to v7.2.1. Use the Syslog format menu to choose formatting.</p>
<b>Use External Database</b>	<p>Check the box to enable use of an external SQL database. Un-check to disable reporting of Bit9 events to the external database.</p>
<b>DSN String</b>	<p>The DSN string that identifies the external database you will be using. This will vary depending upon whether you use manual or NT authentication. The procedure <a href="#">“To enable external event logging to an additional SQL server:”</a> on page 621 describes how to configure these choices.</p>

## Securing Agent-Server Communications

The Bit9 Security Platform uses SSL security for communication between its server and its agents. By default, this is based on a self-signed Bit9 security certificate generated when the Bit9 Server is installed, although a different certificate can be supplied as part of the installation process.

The System Configuration **Security** tab displays the Agent Server Communications configuration page. There, you can make one or more of the following changes:

- If the current certificate for agent-server communications is self-signed, you can edit its details.
- You can import another certificate from a PKCS#12 file, either your own self-signed certificate or from a certificate authority.
- You can increase security by enabling certificate verification so that computers running the Bit9 Agent always verify that the correct certificate is present on the Bit9 Server. This is a one-time change with no reversal. It should only be done for known

certificate authorities – do not enable certificate verification for self-signed certificates.

The screenshot shows a 'System Configuration' window with a 'Security' tab selected. The main section is 'Agent Server Communications Security'. It has a 'Security Status' panel showing 'Certificate Source: Self-signed, no certificate authority', 'Certificate Issuer: bit9srv.mycorp.local', and 'Certificate Verification: Disabled'. Below this is an 'Enable Certificate Verification' button. The 'Current Server Certificate Details' panel contains fields for 'Common Name' (bit9srv.mycorp.local), 'Valid For' (730 days), 'Country Code' (US), 'State' (Massachusetts), 'City' (Waltham), 'Company' (Bit9, Inc.), 'Department' (Support), 'Email Address' (support@mycorp.com), and 'Subject Alternative Name'. There are 'Generate' and 'Cancel' buttons. The bottom panel is 'Import Server Certificate From PKCS12 File' with 'File Name' (Choose File), 'Password', and an 'Import' button.

## Security Status

The top panel of the page shows the security status of agent-server communications. Specifically, it reports on the source of the certificate (self-signed or imported), whether there is a certificate issuer associated with the certificate, and whether the Bit9 Security Platform is configured to require that agents check the server to verify the legitimacy of the certificate. For self-signed certificates, the Certificate Issuer is the name of the Bit9 Server and the certificate has no known certificate authority. This panel also contains the button that enables certificate verification.

## Current Certificate Details

The Current Server Certificate Details panel shows the standard details available from a security certificate. If the certificate is self-signed, you may edit the details and re-generate the certificate.

**To edit the details of a self-signed communications security certificate:**

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click on the **Security** tab. The Agent Server Communications Security page appears.
3. In the Current Server Certificate Details panel, click **Edit**. The fields in the details panel are activated for editing, and the Edit button is replaced by Generate and Cancel buttons.
4. Change certificate details changes as you choose, then click **Generate** to generate a certificate with the new details. To cancel the changes, click **Cancel** instead.

**Table 100:** Agent-Server Communications Certificate Details

Field/Button	Description
<b>Common Name</b>	This must be the fully qualified domain name of the Bit9 Server to which your agents are connected.
<b>Expiration Date/ Valid For</b>	Shows the date and time when the certificate will expire. When you are editing the certificate details, this field changes to <b>Valid For</b> and provides box in which you can enter the number of days or years you want the certificate to be valid.  <b>Note:</b> You cannot enter a Valid For period longer than 20 years or 7300 days for a self-signed certificate.
<b>Country Code</b>	Standard two-letter country code for organization responsible for the certificate.
<b>State</b>	State (if applicable)
<b>City</b>	City
<b>Company</b>	Company responsible for the certificate
<b>Department</b>	Department (if any) within the company
<b>Email Address</b>	Contact information for anyone needing more information about the certificate.
<b>Subject Alternative Name</b>	Subject Alternative Name (SAN) is an alternative means of verifying the certificate against the server hostname. SAN allows the use of multiple DNS names and/or IP addresses, separated by commas, for a single server so that the certificate can be verified even when there is access from different network routes or the same certificate can be used on multiple servers.  The Subject Alternative Name field is empty by default. A tooltip shows the required format. The following is an example of the format for a SAN entry:  DNS=bit9platform.mycorp.com, DNS=bit9platform.mycorp.local,IP=10.0.8.123  You can use wildcards in a DNS name (e.g., *.mycorp.com).

## Verifying that the Server Name and Certificate Match

How the agent verifies that the server name matches the certificate depends upon the server information provided by the server certificate:

- If there are Subject Alternative Name (SAN) DNS entries in the certificate, these are compared to the server address used by the agent, and the two must match.
- If there are no SAN DNS entries, the server address used by the agent is verified against the Common Name (CN) in the server certificate and the two must match.

Mismatches in address/name format between the agent and the server certificate will fail, even if the name resolves to the IP address. For example, where the agent is using an IPv6 address and the SAN is not, verification will fail. You can correct this problem by adding an additional address (the IPv6 address) to the SAN, in the format DNS=[IPv6].

## Importing a Certificate

You can import a new SSL certificate if you choose. Keep the following in mind when planning to import a certificate:

- You cannot import an expired certificate.
- Only PKCS#12 certificates are supported. You cannot use another PKCS version. To use a certificate in another format, you must convert it to a PKCS#12 file format first.
- When you import a certificate, the Edit button is removed from the Current Certificate Details panel since the imported certificate cannot be edited.
- The Bit9 Security Platform supports use of multi-level certificates. The actual certificate must be specified *last* in the PKCS#12 container file.
- Only a certificate matching the Bit9 Server hostname or IP address may be imported.

### Note

During Bit9 Server installation, you must either generate a self-signed certificate or import a real certificate for Bit9 Console. If you import a real certificate, you may use the same certificate for the Agent-Server communications. If you choose this option, you do not need to complete the following procedure.

### To import a new certificate for agent-server communications security:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Security** tab. The Agent Server Communications Security page appears.
3. In the Import Server Certificate panel, click **Browse** to navigate to the location of your new certificate file, and when you locate the file in the Chooser dialog, click **Open**.
4. Enter the Password for the certificate file.
5. When you have provided the necessary information, click **Import**. A dialog box appears describing the impact of the change.

6. To complete the certificate import, click **OK** on the confirmation dialog. A status message reports on the success or failure of the import. If successful, the new certificate is installed in the certificate repository and all fields in the Current Server Certificate Details panel are updated.

## Enabling Certificate Verification

Enabling certificate verification instructs all Bit9 Agents to verify the authenticity of the Bit9 Server certificate against a Certificate Authority or their Root certificates. This adds a level of security to communications because communications between agent and server cannot be spoofed.

### Important

Once certificate verification is enabled, it cannot be revoked, so be certain you have the certificate you want in place and you are sure you want to implement the feature before you click the button. Self-signed certificates were not generated by a known certificate authority, so certificate verification should not be used in that case.

#### To enable verification of the communication certificate on the server by agents:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Security** tab. The Agent Server Communications Security page appears.
3. Make any changes you intend to make to the certificate, whether it is editing the details of a self-signed certificate or importing a new one from a file.
4. In the Security Status panel, click **Enable Certificate Verification**. If you are sure you want to make this change, click **OK** in the confirmation dialog; this cannot be undone in the Bit9 Console. When you click OK, the Enable Certificate Verification button disappears, and the Certificate Verification field changes to *Enabled*.

## Advanced Configuration Options

The Advanced Options tab on the System Configuration page includes options related to database backup, computer and agent management, certificate and updater rules, and general console management. It may also include settings for optional features.

For information about Database Backup options, including backup and restore instructions, see [“Backing Up the Bit9 Server”](#) on page 631 and [“Restoring the Bit9 Server”](#) on page 634.

This section provides a basic description of the other Advanced Options. [Table 101](#) describes the parameters on this page, except for the Database Backup parameters, which are described in the sections referenced above.

**To view and edit Advanced configuration options:**

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Advanced Options** tab. The Advanced Options configuration page appears:

The screenshot shows the 'System Configuration' window with the 'Advanced Options' tab selected. The window has a dark header with a question mark icon. Below the header is a navigation bar with tabs: General, Events, Security, **Advanced Options**, Mail, Licensing, External Analytics, and Connectors. The main content area is titled 'Advanced Options' and contains several sections:

- Database Backup:** Backup Type: Network (dropdown), Backup Path: (text input), Username: (text input), Password: (password input), Windows Domain: (text input), Enabled: , Status: Idle.
- Bit9 Agent:** Automatic Agent Upgrades: Disabled (dropdown), Full OS Inventory Tracking:  Track inventory for locally approved support files signed by "Microsoft Windows" or "Microsoft Corporation" publishers.
- Bit9 Console:** Log Users Out After: 120 (text input) Minutes, Files To Ignore: (text input).
- API:** API Access Enabled: .
- File Uploads:** Delete Uploaded Files After:  after 4 (text input) Week(s), Default Upload Location: files\ (text input) with a Test button.
- Old Computer Cleanup:** All Computers:  delete after 30 (text input) Day(s) offline, Computers Matching Filter:  delete after 30 (text input) Day(s) offline.
- Software Rule Options:** Updaters:  Automatically update application updaters from Bit9 Software Reputation Service, Event Rules:  Process event rules, Indicator Sets:  Automatically update from Bit9 Software Reputation Service, Health Indicators:  Automatically update from Bit9 Software Reputation Service.
- Certificate Options:** Expired Certificates:  Allow approval of software with expired certificates, Exclude Publisher Approvals With These Certificate Algorithms:  MD2RSA  MD5RSA  SHA1RSA  SHA256RSA, Minimum Certificate Key Size For Approval: 512 (dropdown), Digital Signatures:  Require countersignature, Initial Revocation Check: Network (dropdown) Check for revocation on file discovery, Background Revocation Check: Network (dropdown) Check for revocation every 24 hours.

At the bottom of the window are three buttons: Edit, Update, and Cancel.



3. If you need to change any of the configuration information, click **Edit** and make any changes necessary.
4. To submit changes, click the **Update** button and click **Yes** on the confirmation dialog.

**Table 101:** Advanced (Configuration) Options

Section:Field	Description
<b>Database Backup</b>	See <a href="#">“Backing Up the Bit9 Server”</a> on page 631 for a description of these options.
<b>Bit9 Agent: Automatic Agent Upgrades</b>	When <b>Enabled</b> , Bit9 Agents are notified when a new agent version is available, <i>if</i> the Policy the agent is a member of also has agent upgrades activated. It normally is <b>Disabled</b> and is for use during a Bit9 Server upgrade. It has no effect on a new Bit9 Server installation. See the <i>Installing Bit9 Server</i> guide for full instructions on agent upgrades.
<b>Bit9 Agent: Full OS Inventory Tracking</b>	If the box is checked, all files from Microsoft are tracked in the file inventory for this server. If unchecked, locally approved support files whose publisher is “Microsoft Windows” or “Microsoft Corporation” are not tracked in the Bit9 database, which can significantly reduce the load on the server. See <a href="#">“Excluding Tracking of Microsoft Support Files”</a> on page 198 for details.
<b>Bit9 Console: Log Users Out After</b>	Time period of no activity after which a user is automatically logged out the Bit9 Console.
<b>Bit9 Console: Files to ignore</b>	Files that you want to exclude from the Files page lists, separated by commas with optional wildcard character (*). Events associated with ignored files still appear in the Events table and can trigger alerts. Ignored files can be located as Find Files results. Not normally used in normal Bit9 Server operation.
<b>API</b>	If <i>API Access Enabled</i> is checked, the Bit9 APIs are made available on this server. Bit9 APIs allow access to the Bit9 Platform and its database via automation and scripting using a variety of languages. See <a href="#">Appendix B, “Bit9 API,”</a> for details.
<b>File Uploads</b>	(Optional) Settings for the separately licensed feature for uploading files from agent computers. Determines the location to which files are uploaded and the length of time they remain on the server before deletion. See <a href="#">“Uploading Files from Agents”</a> on page 747 for more details.
<b>Old Computer Cleanup: All Computers</b>	Period of time offline after which <i>any disconnected computer</i> is deleted from the list of computer managed by the Bit9 Security Platform. Check the box to activate cleanup, and enter the number of days offline after which a computer will be deleted.  If you reconnect a deleted computer and the computer is still running Bit9 Agent, the computer will resync its file list and return to its last configured policy (if available) or the Default Policy. See <a href="#">“Deleting Computers”</a> on page 146 for more details.

Section:Field	Description
<b>Old Computer Cleanup: Computers Matching Filter</b>	<p>A filtered version of automatic deletion of computers from the list of Bit9-managed computers after a certain period of time. Check the box to activate cleanup, and enter the number of days offline after which a computer will be deleted.</p> <p>You also add one or more filters to limit deleted computers to those matching criteria you specify. For example, you can delete only virtual computers when they reach the time limit. Or you can delete all computers matching a particular tag (e.g., "Visitor"). The filter options are:</p> <ul style="list-style-type: none"> <li>• Computer name</li> <li>• Computer tag</li> <li>• IP Address</li> <li>• Identifier (MAC address)</li> <li>• Parent Template</li> <li>• Platform</li> <li>• Policy</li> <li>• Virtualized</li> <li>• Virtual Platform</li> </ul> <p>Computers must match all filter criteria to be deleted.</p>
<b>Software Rule Options: Updaters</b>	<p>If <i>Automatically update application updaters from Bit9 SRS</i> is checked, Bit9 SRS keeps the Updaters list in the Software Rules section on your Bit9 Server up-to-date with any new versions it confirms.</p> <p>If not checked, the updaters listed continue to be those provided at server installation time, supplemented by any updaters you have manually defined.</p>
<b>Software Rule Options: Event Rules</b>	<p>If <i>Process event rules</i> is checked (the default), events matching rules defined and activated on the Event Rules page can trigger actions such as file analysis or file banning. See <a href="#">"Event Rules"</a> on page 423 for more details.</p>
<b>Software Rule Options: Indicator Sets</b>	<p>If <i>Automatically update from Bit9 Software Reputation Service</i> is checked (the default), Bit9 SRS keeps the Indicator Sets used for threat detection up-to-date. See <a href="#">Chapter 20, "Advanced Threat Detection,"</a> for more on Indicator Sets.</p>
<b>Software Rule Options: Health Indicators</b>	<p>If <i>Automatically update from Bit9 Software Reputation Service</i> is checked (the default), Bit9 SRS downloads Health Indicators used to monitor and report on system health and updates them when necessary. If not checked, the System Health feature is not available. See <a href="#">Chapter 24, "Monitoring System Health,"</a> for more on health indicators.</p>
<b>Certificate Options: Expired Certificates</b>	<p>If <i>Allow approval of software with expired certificates</i> is checked, an expired certificate may be used for publisher-based approval of a file, if the certificate was valid and the certificate timestamp is within the period during which it was valid. See <a href="#">"Approval with Expired Certificates"</a> on page 244 for more details.</p> <p>If not checked, software with expired certificates cannot be approved by publisher.</p>

Section:Field	Description
<b>Certificate Options: Exclude Publisher Approvals With These Certificate Algorithms</b>	<p>This option determines which certificates are <i>excluded</i> from use for publisher approvals. If the box for a certificate algorithm is checked, files signed by a publisher whose certificate uses that algorithm cannot be approved by publisher. See <a href="#">“Excluding Certificate Algorithms”</a> on page 245 for more details.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• MD2RSA</li> <li>• MD5RSA</li> <li>• SHA1RSA</li> <li>• SHA256RSA</li> </ul>
<b>Certificate Options: Minimum Certificate Key Size For Approval</b>	<p>This option specifies a minimum key length for a certificate to be used for file approval by publisher. Certificates whose key size is greater than or equal to the chosen value may be used for approval by publisher. Certificates whose key size is smaller than the chosen value may not be used. The default value is <b>512</b>. See <a href="#">“Minimum Key Size”</a> on page 245 for more details.</p>
<b>Certificate Options: Digital Signatures</b>	<p>If <i>Require countersignature</i> is checked, a countersignature is required for the digital signature of each certificate used to identify a publisher. See <a href="#">“Countersignature Options”</a> on page 245 for information that may assist you in configuring this option.</p>
<b>Certificate Options: Initial Revocation Check</b>	<p>Determines whether and how a certificate revocation check is done at initial file discovery on an agent. There are three possible values:</p> <ul style="list-style-type: none"> <li>• <b>Network</b> – If revocation information is not locally available then use the network to retrieve a certificates revocation status.</li> <li>• <b>Cache</b> – Use locally available revocation status information when performing certificate revocation (the network will not be used).</li> <li>• <b>None</b> – Do not perform certificate revocation checking.</li> </ul> <p>Consider your agent deployment scenario when setting these values since they can impact agent performance. See <a href="#">“Revocation Checks”</a> on page 245 for more details.</p>
<b>Certificate Options: Background Revocation Check</b>	<p>Determines whether and how certificate revocation checks are done for existing files on an agent every 24 hours. If activated, these checks are done in the background. The possible values are the same as those for Initial Revocation Check (above). See <a href="#">“Revocation Checks”</a> on page 245 for more details.</p>

## Backing Up the Bit9 Server

If your SQL Server administrator has a standard backup plan and mechanism, Bit9 recommends that you use that mechanism to backup the Bit9 database.

In case you do not have or choose not to use a separate database backup mechanism, Bit9 provides a mechanism to fully back up and restore the Bit9 Security Platform system as currently configured, including computer configuration, system settings, file database, and event log. The Bit9 backup mechanism backs up all database changes within 6 hours of a critical change, such as a change in policy. Full backups occur once a day. Continuous

automated backups ensure that the server and connected computers remain synchronized after you restore your backup configuration.

The free space available to the backup folder should be at least twice the size of the Bit9 Server database. For both your backup folder and your main SQL database, you should monitor your disk space regularly to prevent overruns.

The Bit9 Server Backup function requires that **xp\_cmdshell** support be enabled on the SQL Server instance where the Bit9 database is hosted. See your SQL Server documentation for instructions on enabling xp\_cmdshell. The following links provide some information about this task:

- SQL Server 2008: <http://www.mssqltips.com/sqlservertip/1673/where-is-the-surface-area-configuration-tool-in-sql-server-2008/>
- SQL Server 2012: <http://msdn.microsoft.com/en-us/library/ms190693.aspx>

### Important

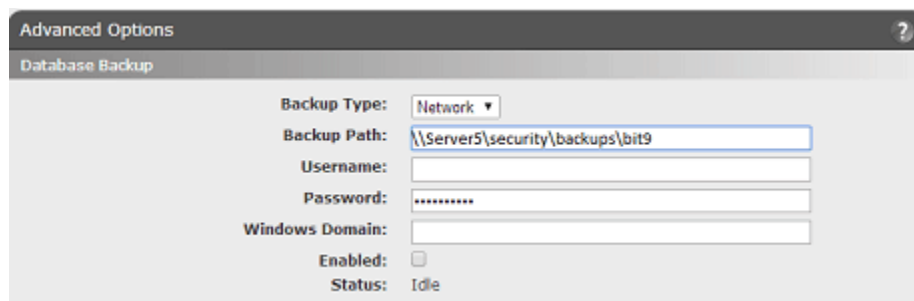
Because enabling xp\_cmdshell has security implications, the SQL Server administrator at your site should follow all best practices to limit any exposure it creates. This includes, but is not limited to, these recommendations:

- Never grant access to non-sysadmin principals.
- Ensure that the sysadmin SQL Server right is granted only to trusted administrators of the SQL Server system.

If you stop using the Bit9 backup mechanism, disable xp\_cmdshell.

### To use the Bit9 Security Platform database backup mechanism:

1. Make sure xp\_cmdshell is enabled on your SQL Server.
2. On the console menu, choose **Administration > System Configuration**.
3. Click the **Advanced Options** tab. The Advanced Options page appears, with the Database Backup panel at the top.
4. Click the **Edit** button at the bottom of the page, and specify backup location and configuration options (see [Table 102](#)):



- Click the **Update** button and then click **Yes** on the confirmation dialog. Each time you save the backup configuration with backup enabled, the Bit9 Server tests backup settings and displays an error message if the configuration fails. The server also writes messages to the Events page that inform you about backup success, problems, or failure.

**Table 102:** Database Backup Options

Field	Description
<b>Backup Type</b>	Network or Local. Local backups should only be used on a different physical drive than the Bit9 Server drive.
<b>Backup Path</b>	<p>The full path to the computer or storage media that will store the backup of the Bit9 database and configuration. Secure your backup directory and ensure that only Bit9 Server administrators have access to it. For best performance, avoid creating unnecessary subdirectories and keep the backup directory as close as possible to the server root directory. For example:  <code>\\server_name\bit9_backup</code></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Local paths are recommended for local backups. You may use a UNC path (the format above) for a Local drive, but the local option does not include username, password, or Windows domain information and no privileges will be used to establish this path.</li> <li>If Bit9 Server is connected to a remote database, the backup path you provide is relative to the database server, and the Username, Password, and Windows domain fields will not appear.</li> </ul>
<b>Username</b> (Network backups)	User name with write permission to the network backup directory.
<b>Password</b> (Network backups)	Domain password for the user account that writes to the network backup directory. For security, your password is encrypted in the Bit9 database.
<b>Windows domain</b> (Network backups)	Windows domain to which the user account for the network backup location belongs.
<b>Enabled</b>	<p>Check the box to begin backups at two-minute intervals to the specified storage location.</p> <p>Clear the checkbox to discontinue automatic backups.</p>
<b>Status</b> (read only)	Time of the next scheduled backup, or status of the most recent backup (including any errors).

**Important**

After you configure the backup directory, do not add, delete, or edit any of its files. Because updating is continuous, such changes adversely affect file synchronization and the integrity of your backup.

## Restoring the Bit9 Server

You can restore the Bit9 Security Platform system to its most recent state. Bit9 database and settings restoration is a manual procedure that requires that you reinstall the Bit9 Server. As a precaution, the Bit9 restoration procedure disables automatic backups to ensure that your only backup copy is not overwritten before you can copy it to a safe location.

The Bit9 Agent runs independently of the Bit9 Server. While you reinstall Bit9 Server and restore the backup configuration, computers remain protected according to the configuration settings received from the Bit9 Server during their last polling instance.

### To restore the Bit9 Security Platform to its most recent configuration:

1. If your Windows installation is corrupted, reinstall the operating system on the Bit9 Server hardware. See the *Installing Bit9 Server* guide for installation guidelines.
2. Reinstall the Bit9 Server:

#### Important

When you reinstall, the IP address of the installation computer is detected. If you installed Bit9 Server using a DNS name, you can sometimes reinstall on a computer with the same name but a different IP address. Otherwise, if you are reinstalling on a computer with a different IP address, you must also reinstall the Bit9 Agent on all computers. Upon installation, computers reinitialize their files and locally approve previously Unapproved files. The restore procedure automatically updates existing agent installation packages to use the new server IP address.

- a. Insert the Bit9 CD (or an executable image of it) in a drive connected to the designated server.
  - b. To run the installer, follow the installation prompts. See the *Installing Bit9 Server* guide for information about installation options, including changing the server IP address, installing via terminal services, or using a DNS name.
  - c. On the Install Type Option screen, select the **Restore from backup** option.
  - d. Navigate to the backup directory.
  - e. Follow the remaining standard installation prompts, and after completing the installation, exit the procedure.
3. During the restoration procedure, continuous backups are automatically disabled. Resume automatic backups as follows:
    - a. Copy all files in the backup folder to a new location so they are not overwritten (or specify a new backup folder and leave existing backup files in place).
    - b. Verify that the currently specified backup directory is now empty so that the fresh backup completes without potential corruption by old files.
    - c. On the Bit9 Console menu, choose **Administration > System Configuration** and then click the **Advanced Options** tab. The Database Backup panel is at the top of the Advanced Options page:

Advanced Options

Database Backup

Backup Type: Network

Backup Path: \\Server5\security\backups\bit9

Username:

Password: .....

Windows Domain:

Enabled:

Status: Idle

- d. Check the **Enabled** check box.
- e. To commence backups in the specified location, click the **Update** button at the bottom of the page and then click **Yes** on the confirmation dialog.

## Configuring Alert and Approval Request Mail

Some Bit9 features require configuration of a mail server so that messages can be sent to administrators or endpoint users under certain conditions. The current features that require this are:

- **Alerts** – email notification of administrators when a Bit9 alert is triggered. See [“Creating Alerts”](#) on page 498 for more information about alerts.
- **Approval Requests** – email notification of a user when their Approval Request is closed. See [“Resolving Requests and Justifications”](#) on page 471 for more information about Approval Request responses.

To enable these email notifications, you must give the Bit9 Security Platform access to an SMTP (Simple Mail Transport Protocol) server to send messages when notification conditions are met. You configure this on the Mail tab of the System Configuration page. There, you can:

- Specify the mail server for notifications.
- Choose standard or secure mail for notifications.
- Enable or disable sending of alert mail to subscribers of specific alerts.
- Specify an optional global subscriber to receive all alert emails.
- Enable or disable automatic delivery of approval request response email.

[Table 103](#) describes all fields for these options.

**Table 103:** Mail Configuration settings

Panel:Field	Description
<b>Alert Settings: Mail Notification Enabled</b>	A checkbox determining whether email subscribers to Bit9 alerts receive email when the alerts are triggered. You might choose to disable this if you are monitoring alerts closely on the Bit9 Console, or are generating a large number of alerts during testing or monitoring activities. Enabled by default.
<b>Alert Settings: Global Subscriber Enabled</b>	A checkbox determining whether a <i>global</i> subscriber to email alerts is enabled. If this is enabled and a subscriber is entered in the Global subscriber field, the subscriber receives email every time any Bit9 alert is triggered. You can enable or disable this as needed.
<b>Alert Settings: Global Subscriber</b>	The email address of the global alert subscriber. Appears only if Global Subscriber Enabled is checked.
<b>Approval Request Settings: Mail Notification Enabled</b>	A checkbox determining whether the user making an Approval Request receives automatic email when the request is closed. Disabled by default.
<b>Server Settings: Mail Server</b>	Mail server address. This can be an IP address or a fully qualified domain name.
<b>Server Settings: Mail Server Port</b>	Port for the mail server. Specify the port in use for your server. Default value of 25 is used for standard SMTP mail; default value of 587 is used for Secure Mail. Make sure the port you use is available for outbound traffic.
<b>Server Settings: Mail "From" Address</b>	Email address used as the <i>from</i> address in notification emails.  The <i>from</i> address need not be an actual, functioning email address, but it must be in the proper syntax for an email address (e.g., info@mycorp.com) or it will generate event log errors. Also, some mail servers automatically discard email without a proper <i>from</i> address as spam.
<b>Server Settings: Secure Mail (TLS)</b>	A checkbox determining whether emails are sent via secure mail. Secure mail requires a username and password to authenticate communication with the email server.  <b>Note:</b> You cannot use Secure Mail with an account that requires multi-factor authentication. Use of such an account will cause Bit9 notifications to fail.
<b>Server Settings: Secure Mail Username</b>	The username for authenticating access to the mail server. Appears only if Secure Mail (TLS) is checked.
<b>Server Settings: Secure Mail Password/ Confirm Password</b>	The password for authenticating access to the mail server. Must be entered in both password fields. Appears only if Secure Mail (TLS) is checked.



Panel:Field	Description
<b>Validate Server: Test Address</b>	An email address used to test your email server configuration. For example, you can use your own email address so that you can click the <b>Send Mail</b> button and immediately know whether the mail server configuration works. The test should be done before the settings on this page are updated so that any issues are exposed and can be remedied.

## Configuring Standard Email for Notifications

To configure email using standard (unsecure) mail:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Mail** tab. The Mail Notification Configuration table appears:

The screenshot shows the 'System Configuration' window with the 'Mail' tab selected. The 'Mail Notification Configuration' panel is active, displaying the following settings:

- Alert Settings:**
  - Mail Notification Enabled:
  - Global Subscriber Enabled:
- Approval Request Settings:**
  - Mail Notification Enabled:
- Server Settings:**
  - Mail Server:
  - Mail Server Port:
  - Mail "From" Address:
  - Secure Mail (TLS):

Please validate settings by sending a test mail before updating the Bit9 Server.
- Validate Server:**
  - Test Address:
  -

At the bottom of the panel are buttons for , , and .

3. Click the **Edit** button to activate the email configuration fields for editing. Fields are added or removed depending upon the options you enable or disable. When you enable an option, required fields for that option appear in red if not filled in.
4. The Alerts Settings Mail Notification Enabled box is checked by default. Leave it checked if you want alert notification emails to be sent.
 

**Note:** See [“Specifying a Global Alert Subscriber”](#) on page 639 before deciding whether to enable a global subscriber.
5. Check the Mail Notification Enabled box in the Approval Request Settings panel if you want automatic email to be sent a requestor when an approval request is resolved.

6. In the Server Settings panel, enter the Mail Server address, either as a fully qualified domain name or IP address.
7. By default, the Mail Server Port defaults to 25 when you use standard mail. If you are using a different port, change the field.
8. Enter a Mail “From” Address. This is the address that recipients will see as the sender of notification email.
9. If you want to use Secure Mail for notifications, provide the information described in [“Configuring Secure Email for Notifications”](#) on page 638.
10. To test the mail server configuration, enter a Test email address at which you can receive mail and click **Send Mail**. The Bit9 Console sends a test email to that address.
11. If the mail server configuration test reported an error in the Validate Server section, correct the problem. The Validate Server test should be successful before you proceed.
12. Click the **Update** button and then click **Yes** on the confirmation dialog. The updated mail configuration is displayed on the Mail Notification Configuration page.

## Configuring Secure Email for Notifications

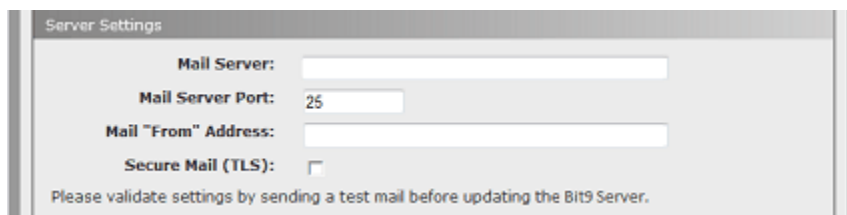
The Bit9 Security Platform provides the option of using a secure mail for Bit9 notifications instead of the standard mail. The secure mail requires a username and password for access to the mail server. Secure mail uses Transport Layer Security, which is an explicit method of securing communication to the mail server. By default, it uses port 587 and initiates the communication with **–BEGINTLS** sent in plain text.

### Important

You cannot use Secure Mail with an account that requires multi-factor authentication. Use of such an account will cause Bit9 notifications to fail.

### To configure the Bit9 Security Platform to use SMTP/TLS for notifications:

1. In the console menu, choose **Administration > System Configuration** and then click on the **Mail** tab. The Mail Notification Configuration page opens.
2. Click **Edit** and check the Secure Mail (TLS) box. Secure mail options appear.



The screenshot shows a 'Server Settings' panel with the following fields and options:

- Mail Server:** [Text input field]
- Mail Server Port:** 25 [Text input field]
- Mail "From" Address:** [Text input field]
- Secure Mail (TLS):**

Below the fields, there is a note: "Please validate settings by sending a test mail before updating the Bit9 Server."

3. If you have not already done so, provide the Mail Server and Mail “From” Address.
4. By default, the Mail Server Port defaults to **587** when you choose Secure Mail. If you are using a different port, change the value in this field.

5. In the Security Mail Username field, provide a username for authentication on the secure mail server.

#### Notes

- For an Exchange Server, the Username should be in the format DOMAIN\username, and the From address field must contain a user email return address.
- For Gmail, the Username should contain the Gmail username without any domain. The value in the From address is ignored.

6. In the Secure Email Password field, enter the password for the mail server username, and enter it again in the Confirm Password field.
7. In the Validate Server panel, enter a **Test Address** and test your mail server settings by clicking on **Send Mail**. If the configuration is valid, a message appears that confirms that the test mail was sent. Check that the mail was received at the address specified.

The screenshot shows a dialog box titled "Validate Server". Inside the dialog, there is a label "Test Address:" followed by a text input field containing the email address "rjones@mycorp.com". Below the input field is a button labeled "Send Mail" with a small envelope icon to its left.

8. When you have confirmed that the email was received as specified, click **Update** to save the configuration, review the changes on the confirmation dialog, and click **Yes** if you are satisfied with the changes.

## Specifying a Global Alert Subscriber

You can designate one user as the global alert subscriber. Because this has the potential to generate a large amount of mail for that user, think carefully before enabling this feature, and consider a special address dedicated to alert tracking. You enable the global subscriber in the Mail Notification Configuration panel of the System Configuration page.

#### To enable one subscriber to receive all alert emails:

1. On the console menu, choose **Administration > System Configuration**.
2. Click the **Mail** tab. The Mail Notification Configuration page appears.
3. In the Settings panel, click **Edit**.
4. Check the **Global Subscriber Enabled** box. The Global Subscriber text box appears.
5. In the Global Subscriber text box, enter the name of the subscriber.
6. Click the **Update** button and then click **Yes** on the confirmation dialog.

#### Note

To disable the global subscriber, *un-check* the Global Subscriber Enabled box and then **Update**.

## Managing Bit9 Platform Licenses

The Licensing panel of the System Configuration page provides the ability to manage Bit9 licenses and to activate, deactivate, and configure Bit9 Software Reputation Service (SRS). The Bit9 SRS options are described in the section “[Activating Bit9 SRS](#)” on page 643.

Bit9 Security Platform can be licensed at two feature levels:

- **Visibility** – Enables all of Bit9’s file and event tracking and reporting capabilities, but does not include control features such as file bans and device blocking.
- **Suite** – Enables both Visibility and Control features.

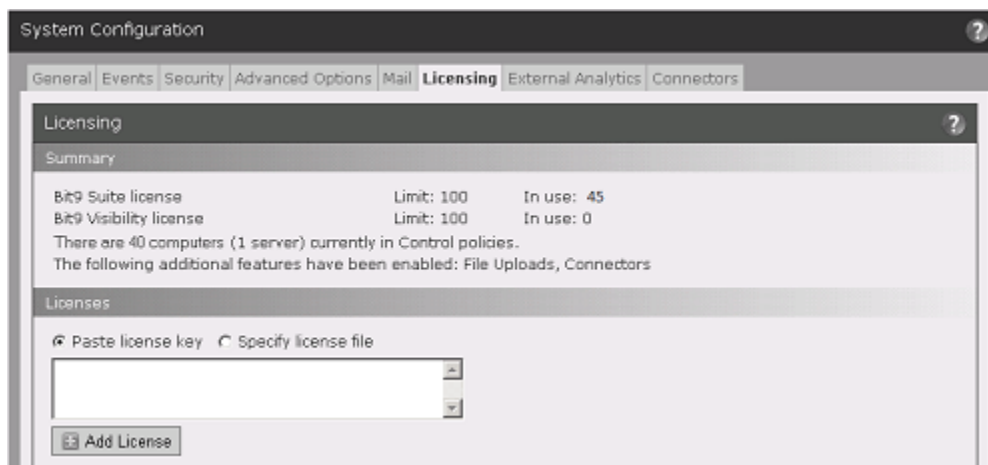
License keys determine the number of agents allowed to run in each mode. You can mix licenses on the same server, having, for example, 20 Visibility licenses and 20 Suite licenses. In addition, you can purchase the Control upgrade at any time to bring the Visibility licenses up to Suite level.

## Viewing Your Bit9 License Limits and Use

The Licensing panel of System Configuration shows the licenses you have at each level, allows you to add new licenses, and shows how many licenses of each type are in use. It also might show that optional or custom features are activated. For example, if you have licensed the Bit9 Connector, it is shown here.

**To view the Bit9 Licensing configuration page:**

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Licensing** tab. The Licensing options appear:



In the Licensing window, the Summary panel shows the following information:

- **Bit9 Suite license** shows the **Limit** for the number of agents (if any) you are licensed to run under full Control mode and the number of these licenses currently **In use**.
- **Bit9 Visibility license** shows the **Limit** for the number of agents (if any) you are licensed to run under Visibility mode only and the number of these licenses currently **In use**.

- **There are  $x$  computer(s) currently in Visibility policies** and **There are  $y$  computer(s) currently in Control policies** not only show the number of systems you currently have in each mode but also provide access to a list of each. When you click the highlighted number in each line, the Computers Page opens showing only the computers in the category you clicked. For example, in the illustration above, clicking on **40** shows a list of computers in Control policies. This line also shows how many computers managed by this Bit9 Server are *servers*.
- If your current license includes optional features, these will also be shown in the Summary panel.

#### Notes

- Bit9 licenses specify the allowable number of agents (computers) in each category; licenses are not locked to particular agents. The number of agents actually operating at each level is controlled by the Mode setting on the Add/Edit Policy page for the policy controlling the agent. You can move a computer or group of computers from Visibility mode to Control mode, or vice versa, as long as you have a sufficient number of Bit9 Suite licenses for the systems in Control.
- For agents in Visibility mode policies, Visibility Only licenses are used first, up to the number you purchased (if any), and then, if necessary, Bit9 Suite licenses are used.

Bit9 Security Platform Administrators can also see licensing information on the Bit9 Console Home Page if the Licensing portlet is displayed. This portlet provides a **Manage your licenses** link that takes you to the Licensing configuration page.

## License Warnings

When you create or edit a policy, or add computers to it, you may change the number of licenses of each type you are using. If the number of agents in Control mode exceeds the number of Bit9 Suite licenses you have, the console displays a warning message. A warning also appears if the total number of agents exceeds the total number of licenses. If you see one of these warnings, take one of the following actions:

- Contact your Bit9 Sales representative to purchase additional licenses.
- Move enough agents out of Control policies to comply with your Bit9 Suite license limit. You can accomplish this by either moving some of your computers to a different policy or by changing one or more policies to Visibility mode.
- Move enough agents to Agent Disabled mode (and uninstall the agent if you do not plan to acquire more licenses) to comply with your license limits.

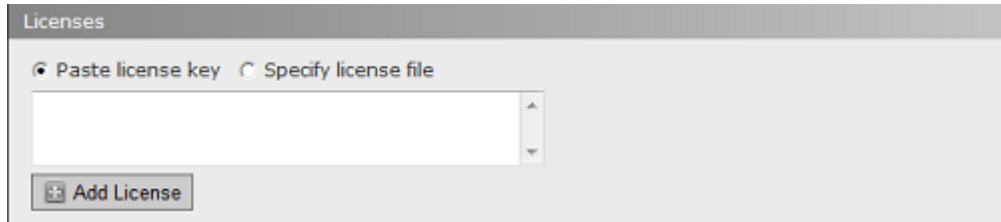
## Adding Licenses

If you acquire a license key for additional agents at either licensing level, you activate the new license on the Licensing page. There are two ways to add a new Bit9 license:

- by entering a string of characters in a text box
- by identifying the location of a file containing the license key

**To add new Bit9 licenses by entering the key:**

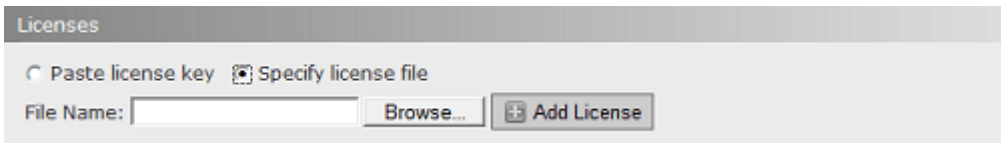
1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Licensing** tab. The Licensing options appear.
3. In the Licenses panel, click the **Paste license key** radio button.



4. Paste or type the license key you received from Bit9 in the text box.
5. Click the **Add License** button.

**To add new Bit9 licenses by filename:**

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Licensing** tab. The Licensing options appear.
3. In the Licenses panel, click the **Specify license file** radio button.



4. Click the **Browse** button to open the file chooser, locate the license file, and click **Open** in the file chooser.
5. Click the **Add License** button.

## Confirming License Addition

If your license addition is successful, the following message will display within the Add License panel: "Bit9 License has been successfully added."

If your license addition is unsuccessful, the following message will display: "Bit9 License has not been added:" along with information about why the addition was unsuccessful. Correct the problem if possible; otherwise, contact your Bit9 Support representative.

## Activating Bit9 SRS

Bit9 Software Reputation Service (SRS) is a web service that provides features to enhance the value of the Bit9 Server. Enabling Bit9 SRS can provide:

- The Software Reputation Service itself, which helps identify and classify software discovered on your computers by comparing it to an extensive database of known files. It provides a threat level and a trust rating to files in its database.
- Bit9 access to your server for remote diagnostics and troubleshooting.
- Cloud-based updates to Trusted Updaters and Advanced Threat Indicators.

While most features are enabled by default when you activate Bit9 SRS, you can opt in or out of feature groups.

### Note

If your Bit9 Security Platform license key included a Bit9 SRS subscription, the key for SRS will already appear on the Licensing page. You will still need to follow the procedure below to accept the terms and conditions of SRS use and activate the service.

### To enable and configure Bit9 SRS:

1. On the console menu, choose **Administration > System Configuration**. The System Configuration page appears.
2. Click the **Licensing** tab. The Licensing configuration options appear, with the Bit9 SRS Activation and Proxy Settings panels at the bottom of the page.

The screenshot shows two panels in a web interface. The top panel is titled "Bit9 Software Reputation Service Activation" and contains the text: "Bit9 Software Reputation Service access has not been activated. If you have a Bit9 Software Reputation Service activation key, enter it below." Below this text is a text input field labeled "Bit9 SRS Key:" and a button labeled "Activate" with a checkmark icon. The bottom panel is titled "Bit9 Software Reputation Service Proxy Settings" and contains an "Enabled:" checkbox (which is currently unchecked), a text input field labeled "URL:", and a button labeled "Test" with a play icon. Below the URL field is the text "Example: http://hostname\_or\_ip[:port]".

3. If you want to use a Proxy Server to communicate with Bit9 SRS, go to the Bit9 SRS Proxy Settings panel, click **Edit**, and configure the settings as described in the table below: See [“Using a Proxy Server for Bit9 SRS”](#) on page 646 if the proxy server requires authentication.

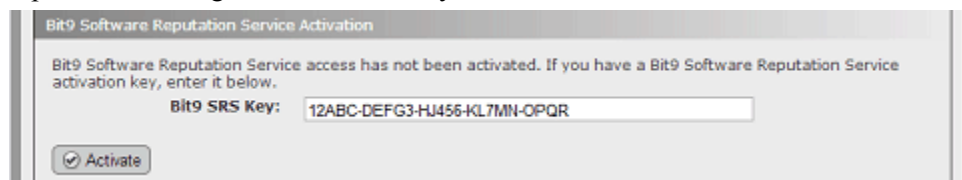
**Table 104:** SRS Proxy Settings

Field/Button	Description
<b>Proxy Settings: Enabled</b>	If checked, use of a proxy server for communication with Bit9 SRS is enabled. You must provide its URL in the URL box.
<b>Proxy Settings: URL</b>	The URL to use as proxy for Bit9 SRS communications. You can use a hostname or an IP address, and optionally add a port specification.

4. Click **Update** and then click **Yes** in the confirmation dialog.
5. If there is already a Bit9 SRS key showing in the Bit9 SRS Activation box, skip to the next step.

- *or* -

If the Bit9 SRS key field is empty, enter the key you have or contact your Bit9 Support representative to get an activation key.



**Note:** Connectivity between the browser and the Bit9 SRS site is required for the remainder of the steps in this procedure.

6. When a Bit9 SRS key is showing, click **Activate**. The Activation panel of the page is updated with new buttons.
7. Click the **Accept Terms and Activate** button. The Bit9 SRS Terms and Conditions page appears in a new browser window.
8. Review the Bit9 SRS terms and conditions. If you agree, check the box to confirm that you have read the terms and click the **Submit** button. This activates your subscription and enables you to connect to Bit9 SRS.
9. Close the Bit9 SRS Activation browser window and return to System Configuration in the Bit9 Console.
10. Click the **Verify Activation** button to determine whether Bit9 SRS was successfully configured for communication with the Bit9 Server.
11. Click the **Options** button, which appears after you complete the activation, to open a web page that allows modification of certain Bit9 SRS parameters. The options include the following checkboxes (note which are enabled by default):
  - **Enable file metadata sharing for Reputation and Threat results from Bit9** – This enables transmission of file metadata (but not file content) collected from your agents to the Bit9 Software Reputation Service for analysis. This option is enabled by default, and keeping it enabled is required for you to have access to the reputation services provided by Bit9.
  - **Enable remote diagnostic analysis by Bit9 Support** – This enables transmission of diagnostic data and aggregate usage information from your Bit9 server to be



sent to Bit9 on an ongoing basis to ensure optimal performance. This is enabled by default.

- **Enable direct file transfer to Bit9 Support for troubleshooting** – This allows any files placed in the Bit9 Server support directories to be sent to Bit9, including log and agent cache files. This helps Bit9 Support respond to questions and issues you report about your Bit9 installation. This option is *not* enabled by default.
- **Enable automatic updates of Trusted Updaters and Advanced Threat Indicators** – This allows Bit9 to remotely update or add trusted Updaters and advanced threat indicators (for detection) on your Bit9 Server. This option is enabled by default.
- **Enable Health Indicators** – This allows Bit9 to remotely deliver Health Indicators, which monitor and report on the health of your Bit9 environment. It also allows updates to existing health indicators. This option is enabled by default. See [Chapter 24, “Monitoring System Health,”](#) for more details on this feature.
- **Enable VirusTotal Lookup** – This integration alerts you to the presence of malware and adware that arrives on endpoints in your environment and which was previously unknown to the SRS. When your Bit9 Platform server looks up newly found hashes in the SRS to get reputation scores, any hashes not known to the SRS are queued for asynchronous lookup in VirusTotal (VT). Any files determined to be malware or adware based on analysis of the VT lookup results are incorporated into the SRS database, and a malicious or potential risk file event is sent down to your platform server.  
**Note:** The SRS does not have access to your actual files and does not upload files for analysis by VirusTotal; only hashes are looked up.

12. Examine the Bit9 SRS Options. If you are unclear on what any option does, contact Bit9 Support for more information. When you know which options you want to enable or disable, click the **Edit Settings** button and check or uncheck the boxes next to each option you want to change. When you are finished, click the **Save Settings** button.

**Note:** You may be prompted to provide your Bit9 Customer Portal login credentials to gain access to the Bit9 SRS Options page. Have these credentials available when you want to view and edit the options.

13. To see the history of Bit9 SRS configuration changes for your server, click the **View Log** link. When you are finished with Bit9 SRS configuration, close the browser window.

Once Bit9 SRS is activated, synchronization of files on your server with Bit9 SRS begins. To initiate a look up of specific files by hash in the Bit9 SRS, you can click the file **Analyze** button from the Files or File Details pages. The analysis results for each file are displayed in a new browser tab. Note that for multi-file requests in Internet Explorer, the popup blocker may block the results for each file after the first one.

## Bit9 SRS Availability Status

Bit9 Server verifies its connection to Bit9 SRS continuously. If Bit9 SRS is not available, an error is displayed on the Licensing tab indicating the reason for the service interruption.

In addition, there is a built-in *Bit9 SRS Unavailable Alert* that is triggered when expected Bit9 SRS tasks are not performed during a period of time specified in the alert (by default, three hours). When triggered, the alert may also send an email notification to a list of alert subscribers.

The three-hour default setting for the Bit9 SRS Unavailable Alert helps eliminate unnecessary alerts for temporary network issues that would be resolved before they would have significant impact on Bit9 SRS users. However, you can change the length of time Bit9 SRS must be unavailable before the alert is triggered. See “Using Bit9 Alerts” on page 494 for more on alerts, including where they are displayed.

Another connection relevant to Bit9 SRS is the connection between the console user’s browser and Bit9 SRS. This connection is required for activation of Bit9 SRS, and also, when you choose Analyze on a Bit9 Console file details page, for redirection to the Bit9 SRS file assessment page. When a user navigates to the Licensing tab, the Bit9 Server checks whether that user can access the Bit9 SRS site and displays the following error if there is a problem with that connection: *Bit9 SRS is currently not accessible. Please check back later.*

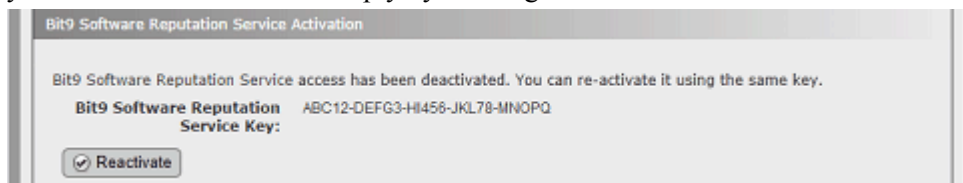
## Deactivating Bit9 SRS

If you need to deactivate Bit9 SRS for some reason, you use the same panel on the System Configuration page Licensing tab that was used for activation.



When you click **Deactivate**, a dialog appears warning that trust and threat information will no longer be provided. You confirm deactivation on that dialog.

The key you previously provided to activate the service is stored so that you can reactivate your Bit9 SRS connection simply by clicking the **Reactivate** button.

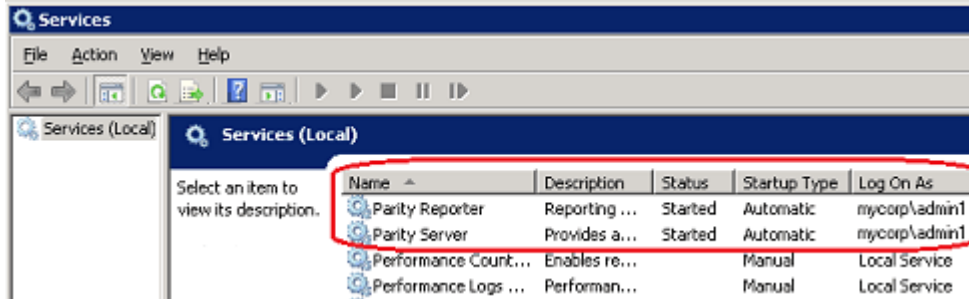


## Using a Proxy Server for Bit9 SRS

You can use a proxy server to handle your communications with the Bit9 SRS. If the proxy server you use does not require authentication, simply provide the URL in the field provided and check the box that activates use of a proxy.

If the proxy server you use requires authentication, you must allow access for the Bit9 Security Platform service user account that was configured during Bit9 Server installation. You can determine the name of this account by opening the Windows Task Manager and

clicking the **Services** button in the bottom right corner. The name in the Log On As field next to Bit9 Reporter must be allowed to access the proxy server.

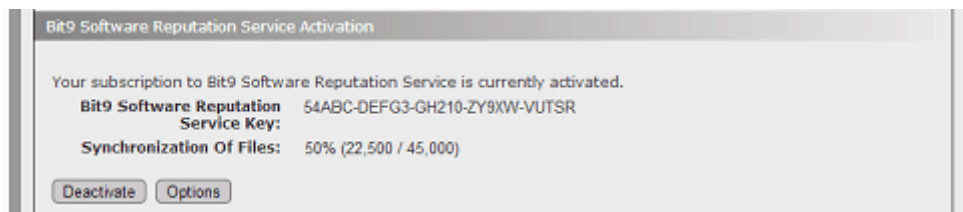


## Bit9 SRS Synchronization

When Bit9 SRS is activated, it begins synchronizing file information with the Bit9 Server. This synchronization allows Bit9 SRS to provide trust and threat levels for files on the server that are also known to SRS. The amount of time this takes depends upon the number of files to be synchronized.

After the initial synchronization, Bit9 SRS and Bit9 Server continue to communicate. New files discovered on the server are synchronized with Bit9 SRS, trust and threat levels are updated when they change, and other file metadata, such as publisher and certificate data, may be updated.

The Bit9 SRS Activation panel provides the status of file synchronization. It includes the total number of unique files found on the server, the number and percent synchronized so far, and the estimated amount of time left before synchronization is complete. This is especially useful during the initial synchronization, but also can be helpful for tracking the availability of trust and threat information on the server when a large number of new files appears on the server.



### Note

The estimate of time to complete synchronization might not be accurate if there are technical difficulties with the database or an interruption in network connectivity to Bit9 SRS. If an error occurs during synchronization, the process is paused temporarily to allow for normal operations to be restored, and an error message indicates the length of the pause.

## Activating Carbon Black Server Integration

If you are managing your endpoints with both a Bit9 Server and a Carbon Black Server, you can configure the Bit9 Server to connect to the Carbon Black Server to receive and display information about files and Carbon Black watchlist events. [Table 105](#) shows the configuration settings for this integration. Carbon Black Server configuration is located on the Licensing tab of the System Configuration page.

**Table 105:** Carbon Black Integration Configuration settings

Field/Button	Description
<b>URL</b>	The URL of the Carbon Black server you want to link to the Bit9 Server. Port is optional.
<b>Validate SSL Certificate</b>	Checking this box causes a validity check on the Carbon Black server certificate. This should be checked only if the Carbon Black server certificate is not signed.
<b>API Token</b>	You enter the API Token here for a Carbon Black server user that will be used for the Bit9 integration. Click the <b>Test</b> button to confirm that the server is accessible and the key works. The test returns one of the following values: <ul style="list-style-type: none"> <li>• <b>Success, version:</b> &lt;Carbon Black product version&gt;</li> <li>• <b>Invalid API Token</b></li> <li>• <b>Server not accessible</b></li> </ul> <b>Important:</b> See <a href="#">“Creating a Carbon Black User for the Integration”</a> for more on this field.
<b>Receive Watchlist Events</b>	Checking this box activates delivery of Carbon Black watch list events from the configured server to the Bit9 Server.
<b>Force Strong SSL</b>	Checking this box causes the Carbon Black server to check the Bit9 Server certificate before sending events. <i>Do not</i> check this box if your server uses a self-signed Bit9 certificate on IIS.

### Important

These settings also appear in the Carbon Black console. Although the Bit9 Platform integration settings in the Carbon Black console allow editing, changes made there will not be applied. Bit9-Carbon Black integration settings should be edited only in the Bit9 Console.

## Creating a Carbon Black User for the Integration

Because you may enter only one API token when configuring the integration between Carbon Black and the Bit9 Platform, you should create a new Carbon Black user for this purpose and use the API Token for that user. The Carbon Black user whose token is used must be in the Administrators group and also must be a Global administrator. The summary of basic steps is shown below:

### To create a Carbon Black - Bit9 Integration user and API Token (summary steps):

1. Login to the Carbon Black server as a user capable of creating other administrative users.
2. In the Carbon Black console, go to **Administration > Users**, click **Add User**, and create the new Bit9 integration user. Be sure to assign this user to the Administrators team and also check the *Global administrator* box.
3. Logout and login to the Carbon Black console again as the new user you created.
4. In the Carbon Black Console menu, choose *username* > **My Profile**.
5. On the My Account page, choose **API Token** on the left menu and copy the string in the **Your API Token** box. This is the string you will use to configure Carbon Black integration in the Bit9 Platform console, on the Licensing tab of the System Configuration page.

See “Integrating Carbon Black with a Bit9 Server” in the *Carbon Black User Guide* for more detailed instructions.



## Chapter 24

# Monitoring System Health

This chapter introduces the System Health page, which provides Bit9 administrators with the ability to monitor the health and performance of the Bit9 Server.

**Sections**

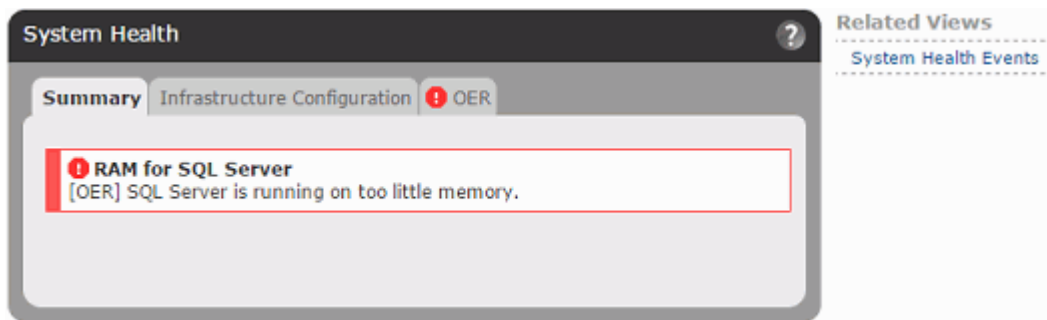
Topic	Page
<a href="#">Overview</a>	652
<a href="#">Enabling System Health Indicators</a>	653
<a href="#">Viewing the System Health Page</a>	654
<a href="#">System Health Alerts</a>	657
<a href="#">System Health Events</a>	658

## Overview

The System Health page provides Bit9 administrators with the ability to monitor factors that affect the performance of the Bit9 Server. It displays the output of *Health Indicators* that can warn you about problems on the Bit9 Server, the SQL Server, or the environment as a whole.

For example, your servers might not be in compliance with the Bit9 *Operating Environment Requirements* guidelines for the number of rules or endpoints being managed. This could occur because you added more endpoints with Bit9 Agents to your environment. Another cause of a system health deterioration might be a change in your hardware environment, such as a change in disk capacity or RAM.

The System Health page can help you see these trends before they become a serious problem, so that you can either remedy them yourself or contact Bit9 Support for guidance. Knowing that all of the monitored factors are healthy can also be helpful.



The System Health page contains different tab views showing the results of analysis by different health indicators. The first tab will show the overall Health Summary, which will include brief headlines for any triggered health indicators. Other tabs contain one or more related indicators. The information on the tabs may be presented as a graph, a table, simple text, or a combination of formats.

Health indicators provide feedback on critical or borderline conditions in several different ways:

- **System Health Page Triggered Indicators** – When an indicator detects that your server has an issue that affects its health, the System Health page displays a red icon and highlighting, as shown above. If a yellow icon and highlighting appears for an indicator, the factor it is reporting on is in a borderline but not critical state.
- **Alerts** – There is a built-in alert for each tab on the System Health page to warn when your system is not in compliance with the Bit9 Platform *Operating Environment Requirements* or other required configuration, and you can also create an alert to be triggered when a health indicator changes its severity level.
- **Events** – When the severity level of a health indicator changes, an event is recorded by the server and made available through Syslog output.

The Health Indicators displayed on the System Health page are delivered to the Bit9 Server through the Bit9 Software Reputation Service (SRS). This cloud service not only delivers the initial set of indicators needed to enable the System Health page but also keeps your server up to date with any changes to existing indicators as well as new indicators that will add to your view of system health. Bit9 SRS must be connected to your server for the System Health indicators to function.



## Enabling System Health Indicators

System health indicators are provided by the Bit9 Software Reputation Service (SRS). The SRS must be enabled for the initial download of Health Indicators from the cloud, and it is also used to update existing indicators when necessary and to add new indicators as they are developed.

In addition to enabling the Bit9 SRS on your Bit9 Server, you must enable Health Indicators “updates” setting on the Advanced Options tab of the System Configuration page. This switch enables both initial downloading and later updates of health indicators.

### To enable System Health Indicators on a Bit9 Server:

1. On the console menu, choose **Administration > System Configuration** and click the **Licensing** tab.
2. On the Licensing tab, check to see whether the Bit9 Software Reputation Service Activation panel shows that the SRS is activated. If it is not activated, follow the activation instructions in [“Activating Bit9 SRS”](#) on page 643.
3. When Bit9 SRS is activated, click on the **Advanced Options** tab on the System Configuration page and click the **Edit** button at the bottom of the page.
4. In the Software Rule Options panel, check the box for **Health Indicators**. When the page is saved, this automatically downloads Health Indicators from the Bit9 SRS and also updates them as necessary.
5. Click the **Update** button at the bottom of the page. Download of the Health Indicators is scheduled and begins shortly. See [“Viewing the System Health Page”](#) for a description of what you will see once this feature has been activated.

Once System Health Indicators have been activated, they begin to download to your server from the Bit9 SRS. Depending upon your connection speed and other server activities, this might take one or two hours.

## Disabling System Health Indicators

If you need to disable Health Indicator updates, go to the System Configuration page Advanced Options tab, click the **Edit** button, uncheck the **Health Indicators** box, and click the **Update** button. When you go to the System Health page after disabling indicators, the page will show a message about the feature not being enabled.

## Viewing the System Health Page

Users must have a login account with “View system health indicators” permission to view this page. Accounts in the Administrators group have this permission by default. See [“Managing Console Account Groups”](#) on page 89 if you need to configure another user for access to this page.

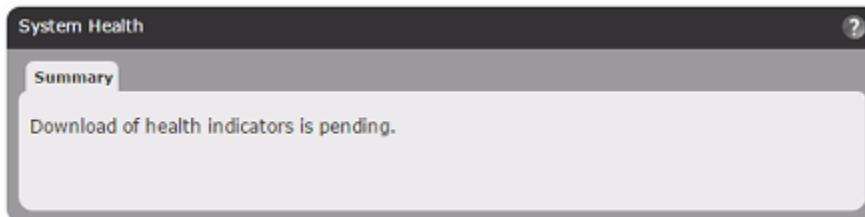
### Note

The System Health page illustrations shown here were accurate at the time of publication, but because Health Indicators are delivered and updated from the Bit9 cloud, the exact indicators on any tab, and their appearance and content on your version of the Bit9 Console, may be different.

### To view the System Health page:

- On the console menu, choose **Administration > System Health**.

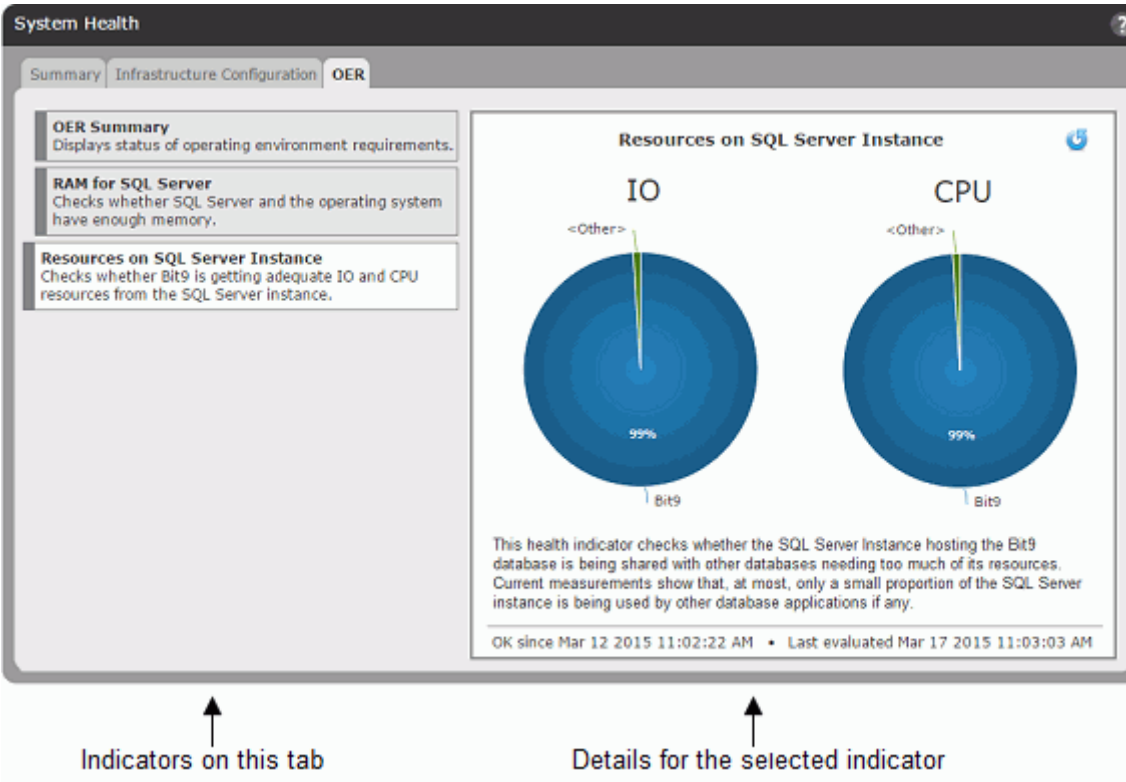
If the initial download of indicators is not complete, only the Summary tab appears on the System Health page, and it displays a message that the download is pending.



When the download is complete, the page has tabs for each of the available health views. The first tab shows the overall health Summary, which will include any triggered health indicators and also report any conditions that prevent proper operation of Health Indicators. The Summary tab also indicates when there are no triggered indicators.



The other tabs show the results of analysis by the different health indicators – these will vary as new indicators are made available through the SRS.



There may be multiple indicators on a System Health tab view, such as in the example above. Indicators are shown on the left side of the page, and the view on the right side of the tab shows the details for the selected indicator, which is offset to the left.


There are several conditions under which no indicators are shown on the System Health page:

- There are no health indicators available because the Bit9 Software Reputation Service (SRS) is disabled.
- The System Health feature not enabled.
- The download of health indicators from SRS is still pending.

## Navigating on the System Health Page

There are several ways to change views or drill down for additional information on the System Health page:

- **Change Tab Views** -- You can click on any of the tabs to change the set of indicators you are viewing.
- **Change Indicator Shown on a Tab** -- If there are multiple indicators on a tab, you can click on one of the other indicators on the left to change to the details shown on the right.
- **Links in the Details** -- Some indicator details include links to additional information. For example, the OER Summary details view includes a link to the current *Operating Environment Requirements* document for the Bit9 Platform on the Bit9 Customer Portal -- note that you must have your portal login to complete navigation to this link.

- **Reload Indicator Details** -- Use the reload button  in the upper right corner of the indicator details view if you want to be certain that you are viewing the most current information. Most indicators are re-evaluated every 24 hours; the OER Summary indicator is re-evaluated every 15 minutes.
- **System Health Events** -- The Related Views menu on the System Health page includes a links to the Events page, filtered to show only events related to health indicators. See [“System Health Events”](#) on page 658 for more about these events.

## Health Indicator State

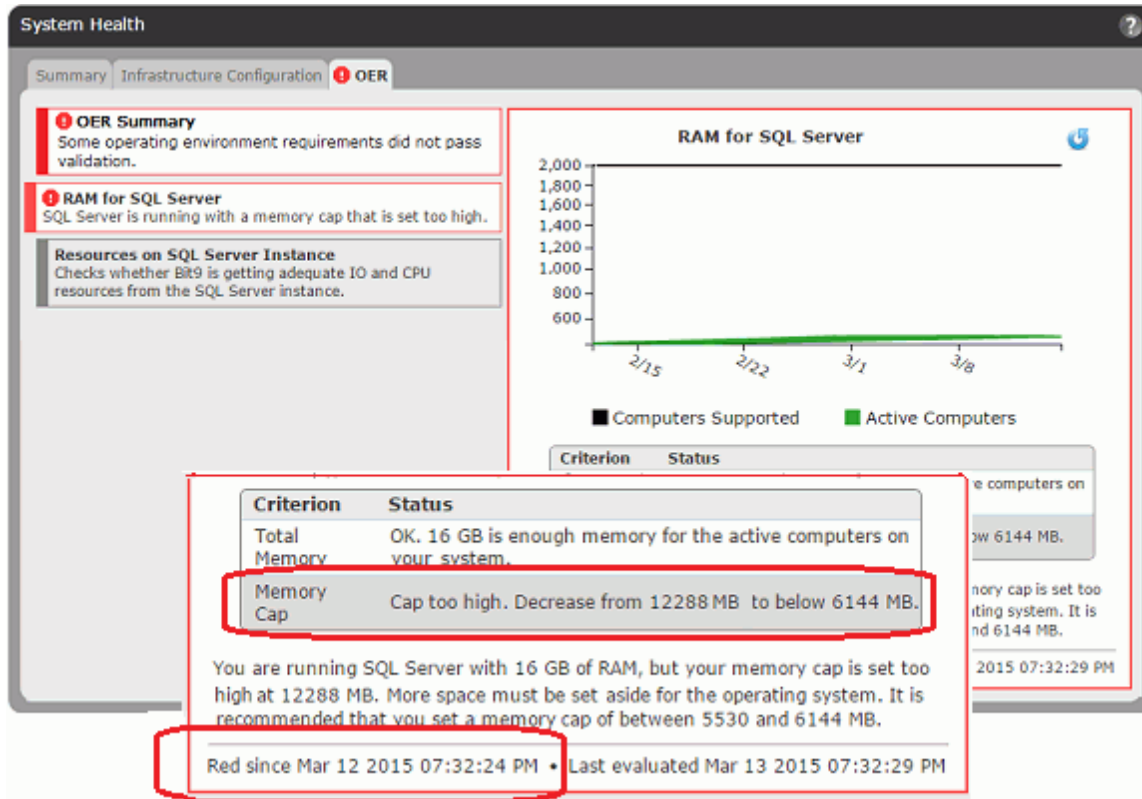
Health indicators are color coded to show the state of the parameter or resource they monitor. The colors and their states are:

- **Gray** -- When an indicator is gray, the condition it is monitoring is healthy (or is strictly informational and does not have a health rating) and no action is required.
- **Yellow** -- When an indicator is yellow, the condition it is monitoring is borderline, and you should follow up and take action if necessary.
- **Red** -- When an indicator is red, the condition it is monitoring is in a critical state and action is required.

### Note

If the Bit9 Server determines that an indicator is not relevant in your environment, that indicator might not be displayed.

When an indicator is showing anything less than a healthy state, it is considered “triggered”, and a triggered indicator shows its state in multiple locations, including the list of indicators on the Summary tab view, and on the tab itself and the list of indicators for the view in which the indicator appears. In addition, a description of the problem and the length of time it has existed appear in the details section of the tab view, and an alert is triggered to warn of the issue.



## System Health Alerts

Alerts can notify you of system health issues. These notifications appear in the Bit9 Console and (if enabled) are emailed to subscribers. See “Using Bit9 Alerts” on page 494 for full details on alerts. These alerts may notify you of system health issues:

- **System Health OER Alert** – This built-in alert displays a console alert and sends emails to any subscribers when the environment for the server is out of compliance with certain specifications in the Bit9 Platform *Operating Environment Requirements*. It is permanently enabled, although it cannot be triggered if Health Indicators are not enabled.
- **System Health Infrastructure Configuration Alert** – This built-in alert displays a console alert and sends emails to any subscribers when any factors reported on the Infrastructure Configuration tab of the System Health page are out of compliance. It is permanently enabled, although it cannot be triggered if Health Indicators are not enabled.

### Note

System Health alerts only appear and can only be triggered if System Health Indicators are enabled on the Advanced tab of the System Configuration page and the related indicator has been downloaded to the server. If present, they are always enabled.

## System Health Events

The Bit9 Server records several different events related to health indicators. You can view these events in the Bit9 Console, set up rules in a SIEM that respond to these events, and trigger Bit9 Alerts or Event Rules based on them. There are event subtypes to inform you of changes in the indicators themselves: *Health indicator created*, *Health indicator changed*, and *Health indicator deleted*.

The event most likely to be of interest for monitoring system health is the *Health indicator severity change* subtype. An event indicating a severity change from lower to higher means that some element in your Bit9 environment needs your attention. On the other hand, a decrease in severity can let you know that a remediation you performed was successful. Increases in severity trigger events whose severity is Warning. Decreases in severity trigger events whose severity is Info.

The Description fields for the severity change event provide details about why the event was triggered. It also includes descriptions of the state of newly created indicators. [Table 106](#) shows the conditions that trigger *Health indicator severity change* events.

**Table 106:** Health Indicator Severity Change Event Conditions

Condition	Description
<b>Indicator condition is no longer healthy</b>	Health indicator <name> has gone to severity <severity level>. Check the health indicator for more details.
<b>Severity increased from yellow to red</b>	Health indicator <name> has increased in severity from <old severity> to <new severity>. Check the health indicator for more details.
<b>Severity decreased to yellow</b>	Health indicator <name> has decreased in severity from <old severity> to <new severity>.
<b>Triggered indicator is now healthy</b>	Health indicator <name> is now healthy.
<b>New indicator condition is unhealthy</b>	Newly created health indicator <name> has severity <severity level>. Check the health indicator for more details.
<b>New indicator condition is healthy</b>	Newly created health indicator <name> is healthy.

### To view health indicator events in the Bit9 Console:

1. On the console Events page, choose **Reports > Events**.
2. In the Saved View menu, choose **System Health History**.
3. Make any other adjustments you choose to the other table view parameters, such as Max Age.

## Appendix A

# Live Inventory SDK: Database Views

In addition to the access provided to the Live Inventory of files and computers through the console user interface, the Bit9 Security Platform provides public views into the database. You can create your own reporting and data analysis solutions through the use of these public views. This appendix describes the available read-only database views.

Creating your own custom reports using the external database views may be useful when you want to perform complex analysis of file and computer inventory data. The SDK also facilitates:

- A special combination of filters or a file grouping not provided in the Bit9 Console.
- Inquiries that perform faster when done through direct database access outside of the console user interface.
- Reports that run on a specific schedule and/or need their output integrated into third-party tools.

### Note

The Bit9 Platform also includes the Bit9 API, a RESTful API that provides programmers a way to write code that interacts with Bit9 Platform, either using custom scripts or from other applications. See [Appendix B, “Bit9 API,”](#) for more information.

## Performance Considerations

The external views provide read-only access to the database and are optimized to not interfere with other Bit9 Server tasks. The database server is a shared resource, however, and overall performance of the Bit9 Server might be affected by extensive querying of external views. Consider the following general suggestions:

- Avoid running queries that take more than two minutes to complete.
- Limit total time spent querying the external database to no more than 5% of total time (e.g., a few minutes each hour).
- If possible, run queries at a time of day when Bit9 Agents are not very active, especially avoiding times when agents are initializing.

Contact Bit9 Technical Support for assistance with performance issues.

## Upgrading from a Previous Version

If you used these database views in a previous release, you may need to modify some queries to match changes in this release. In the tables for each view, changes since Bit9 (Parity) 6.0.2 are indicated in the following ways:

- **New** fields are indicated with a solid delta (▲) next to the name if new for **7.0.0**, a solid diamond (◆) if new for **7.0.1**, and a solid star (★) if new for **7.2.0**. Note that some fields were introduced in different builds or patches of the same version.

- **Changed** fields (field name or its values) are indicated with an open delta symbol ( $\Delta$ ) next to the name if changed for for **7.0.0** and an open diamond ( $\diamond$ ) if changed for **7.0.1**. A **Change Note** in the Comments column describes what has changed. Note that some fields were changed in different builds or patches of the same version.
- **Removed** fields are noted in the introduction to each view table.

Bit9 v7.2.1 supports agent installation on Mac, Linux and Windows computers, so any path-related field will have have operating-system-specific syntax (including delimiters).

In addition, if you are upgrading from v6.0.2 or ealier, you should be aware of the following global changes in terminology, which affect many of the SDK values:

**Table 107:** Global Terminology Changes for Post-6.0.2 Releases

Category	6.0.2 Term	7.2.1 Term
File Status	Pending	Unapproved
	Approved (Custom)	Approved by Policy
	Banned (Custom)	Banned by Policy
Computer protection level	SecCon	Enforcement Level
Enforcement Level value	20-Lockdown	High (Block Unapproved)
	30-Block-and-Ask	Medium (Prompt Unapproved)
	40-Monitor	Low (Monitor Unapproved)
	60-Visibility Only	None (Visibility)
	80-Agent Disabled	None (Disabled)



## Schema Overview: bit9\_public

External views represent a de-normalized view of the Bit9 Server live inventory. These views are suitable for reporting and analysis using data cubes. Each exposed view uses the naming convention with the prefix “Ex” for “external,” and is in the schema **bit9\_public** within the database **Das**.

### Specifying a Schema User

You must provide a login name for the user to whom you want to grant access to the **bit9\_public** schema. Use the following script to add this login name and login manually (after the Bit9 Server is installed). Replace *Domain* and *bit9user* with your own values for the appropriate Windows user:

```
CREATE LOGIN [Domain\bit9user] FROM WINDOWS WITH
DEFAULT_DATABASE=[Das]
GO
CREATE USER [Domain\bit9user] FOR LOGIN [Domain\bit9user]
GO
USE [Das]
GO
GRANT SELECT ON SCHEMA :: dbo TO [Domain\bit9user]
GO
GRANT EXECUTE ON SCHEMA :: dbo TO [Domain\bit9user]
GO
ALTER AUTHORIZATION ON SCHEMA::bit9_public TO
[Domain\bit9user]
GO
```

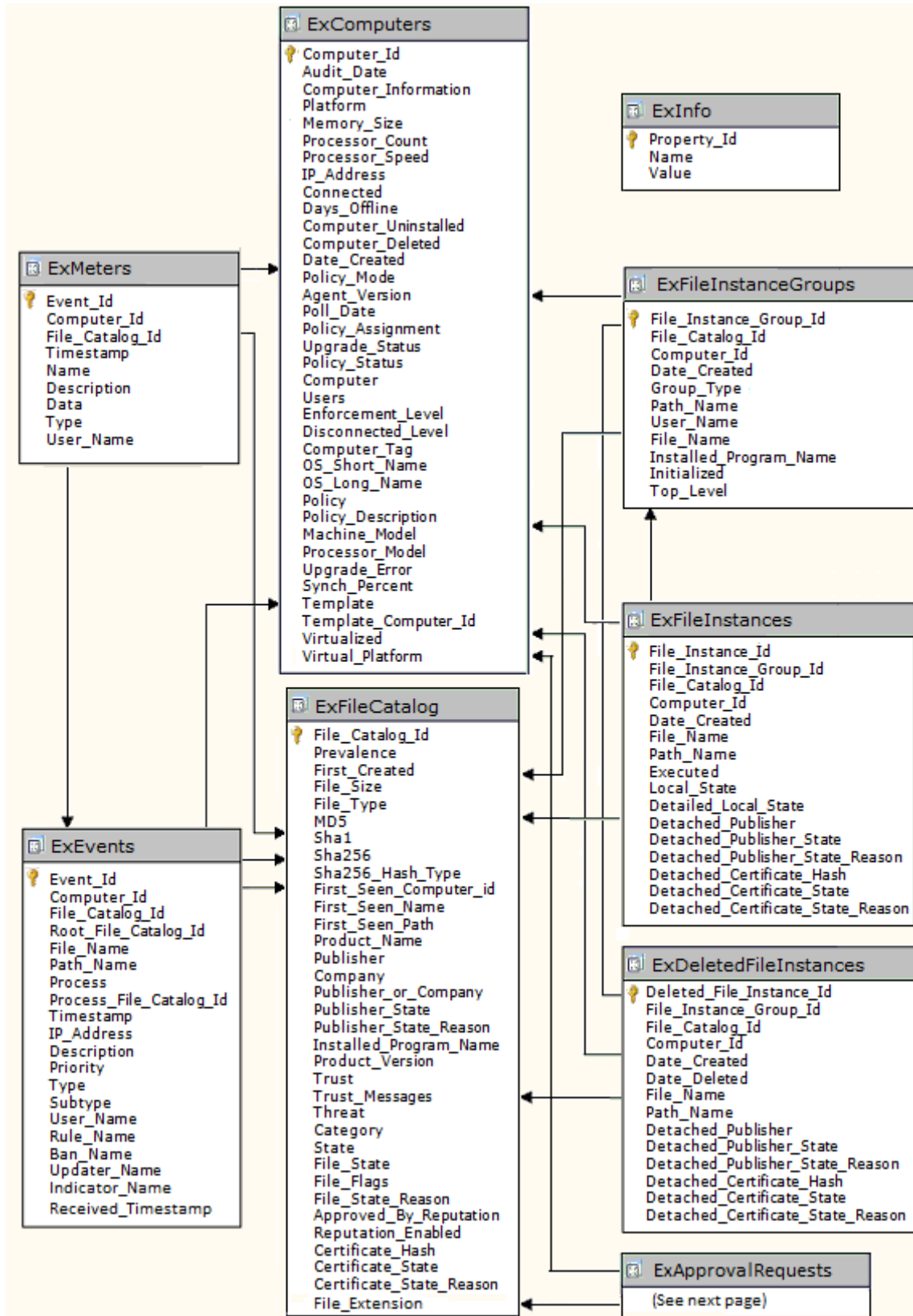
### Schema Views and Diagram

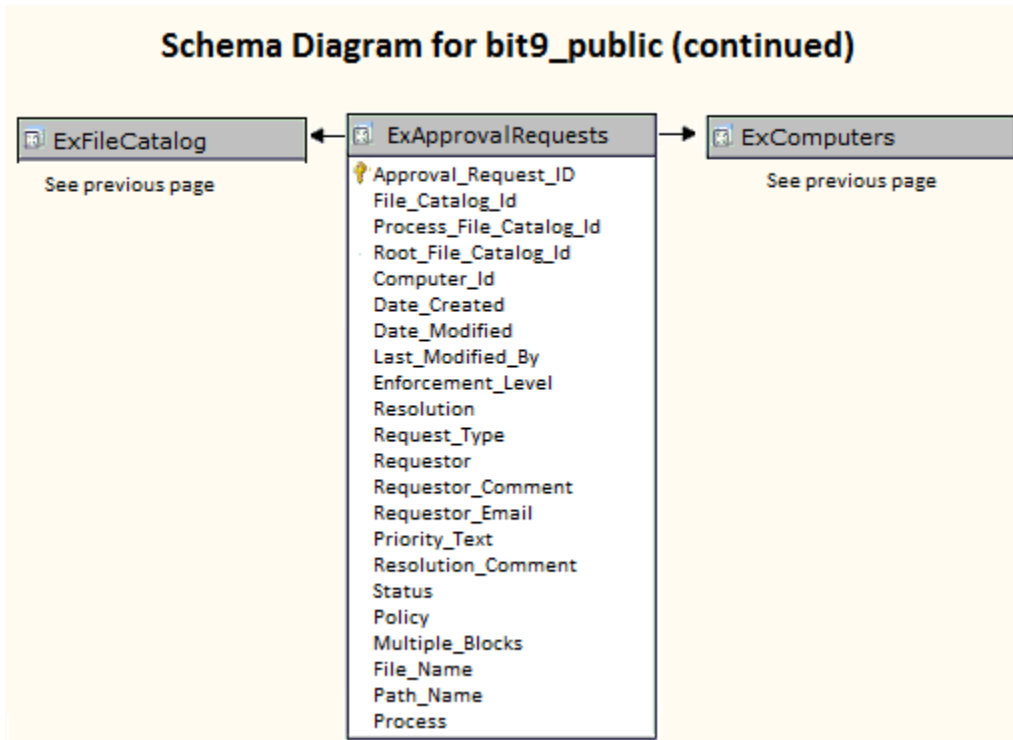
[Table 108](#) shows the views available in the schema. Detail about the data in each view is shown in the subsequent tables in this topic. The full schema diagram for bit9\_public appears immediately after the table.

**Table 108:** Schema Views for bit9\_public

View Name	Description	Primary Key	Foreign Keys
ExInfo	Public properties of servers and schema in the Bit9 Server environment	Property_Id	(None)
ExEvents	All events shown on the Events page	Event_Id	File_Catalog_Id, Root_File_Catalog_Id, Computer_Id
ExMeters	All executions of metered files	Event_Id	Computer_Id, File_Catalog_Id
ExComputers	Metadata of all computers	Computer_Id	(None)
ExFileCatalog	Metadata for all unique hashes	File_Catalog_Id	(None)
ExFileInstances	Metadata of all file instances on all computers	File_Instance_Id	File_Instance_Group_Id, Computer_Id, File_Catalog_Id
ExDeletedFileInstances	Metadata of all deleted file instances	Deleted_File_Instance_Id	File_Instance_Group_Id, Computer_Id, File_Catalog_Id
ExFileInstanceGroups	Metadata of all file instance groups	File_Instance_Group_Id	Computer_Id, File_Catalog_Id
ExApprovalRequests	All approval requests shown on the Approval Requests page	Approval_Request_Id	File_Catalog_Id, Process_File_Catalog_Id, Root_File_Catalog_Id, Computer_Id

## Schema Diagram for bit9\_public





## Details of Database Views

### ExComputers

The ExComputers view provides access to the metadata of all computers running the Bit9 Agent at your site. To see a list of this data for all computers in the Bit9 Console, choose **Assets > Computers** the console menu. To see this data for a single computer, click on the name of a computer on the Computers page.

**Table 109:** ExComputers View Details

Field Name	Data Type	Special Values	Comments
<b>Computer_Id</b>	<b>int</b>		<b>Primary key</b>
Audit_Date	nvarchar		Date and time when Computer Information was collected
Computer_Information	XML		A meta-field containing data (in XML format) about the computer including number of drives and free space on each; number, model and speed of processors; and total RAM on system.
▲ Platform	varchar	'Windows', 'Mac', 'Linux'	
Memory_Size	int		Size (megabytes) of installed memory on this computer
Processor_Count	int		Number of processors on this computer
Processor_Speed	float		Speed of computer processor in MHz
IP_Address	varchar		Last recorded IP address of this computer. This can be either an IPv4 or IPv6 address.
Connected	varchar	'Yes', 'No'	'Yes' if agent on this computer is connected to the Bit9 Server
Days_Offline	int		Number of days this computer has been offline
Computer_Uninstalled	varchar	'Yes', 'No'	'Yes' if agent has been uninstalled from this computer
Computer_Deleted	varchar	'Yes', 'No'	'Yes' if computer has been deleted from the Computers list in the Bit9 Server
Date_Created	datetime		Date and time this computer first connected to the Bit9 Server
Policy_Mode	varchar	'Control', 'Visibility', 'Agent Disabled'	Mode of the policy this computer belongs to
Agent_Version	varchar		Version of the agent installed on this computer

Field Name	Data Type	Special Values	Comments
Poll_Date	varchar		Date and time this computer last connected to the Bit9 Server
Policy_Assignment	varchar	'Manual', 'Automatic'	How policy is assigned to this agent (automatic means it was assigned by Active Directory mapping)
Δ Upgrade_Status	varchar	'Up to date', 'Completed', 'Not supported', 'Scheduled', 'Waiting', 'Not requested', 'Agent uninstalled', 'Reboot required', 'Blocked', 'Upgrade requested', 'Unknown'	Current upgrade status of this agent <b>Change Note:</b> 'Upgrade requested' was added in 7.0.0.
Δ Policy_Status	varchar	'Policy out of date', 'Approvals out of date', 'Enforcement Level out of date', 'Out of date', 'Up to date'	Current policy status of this computer <b>Change Note:</b> Value 'Enforcement Level out of date' was 'SecCon out of date' in 6.0.2.
Computer	nvarchar		Name of this computer
Users	nvarchar		Comma-separated list of users that have ever logged on to this computer
Δ Enforcement_Level	nvarchar	'High (Block Unapproved)', 'Medium (Prompt Unapproved)', 'Low (Monitor Unapproved)', 'None (Visibility)', 'None (Disabled)'	Enforcement Level used when this computer is online <b>Change Note:</b> Enforcement_Level was Online_SecCon in 6.0.2. All values changed beginning with 7.0.0.
Δ Disconnected_Level	nvarchar	'High (Block Unapproved)', 'Medium (Prompt Unapproved)', 'Low (Monitor Unapproved)', 'None (Visibility)', 'None (Disabled)'	Enforcement Level used when this computer is offline <b>Change Note:</b> Disconnected_Level was Offline_SecCon in 6.0.2. All values changed beginning with 7.0.0.
Computer_Tag	nvarchar		Optional custom tag assigned to this computer
OS_Short_Name	nvarchar		Short name of the OS installed on this computer
OS_Long_Name	nvarchar		Long name of the OS installed on this computer
Policy	nvarchar		Name of the last policy this agent has joined

Field Name	Data Type	Special Values	Comments
Policy_Description	nvarchar		Description of the last policy this agent has joined
Machine_Model	nvarchar		Machine model of this computer
Processor_Model	nvarchar		Processor model of this computer
Upgrade_Error	nvarchar		Agent upgrade error (if any)
Synch_Percent	int		Progress of synchronization of this computer with the Bit9 Server (percent)
▲ Template	varchar	'Yes','No'	'Yes' if computer is a template. 'No' if it is not (includes clones and non-cloned computers).
▲ Template_Computer_Id	int		The ID of the parent template computer. If the value is 0, the computer does not have a template parent and is not a clone. If the value is non-zero, the computer is a clone.
▲ Virtualized	varchar	'Yes','No'	'Yes' if computer is a virtual machine. 'No' if it is not.
▲ Virtual_Platform	varchar		If Virtualized is 'Yes', the platform of the virtual machine. Currently, this will be either 'VMware', 'Unknown', or blank.

## ExInfo

The ExInfo view provides access to data about the Bit9 Server and public schema (this schema) versions as well as the address of the Bit9 Server and other servers in its environment.

**Table 110:** ExInfo View Details

Field Name	Data Type	Special Values	Comments
<b>Property_Id</b>	<b>int</b>		<b>Primary Key</b>
Name	nvarchar	'RPCServerAddress', 'Bit9ServerVersion', 'WebServerAddress', 'DBPublicSchemaVersion',	Name of the property
Value	nvarchar		Value of the property

## ExMeters

The ExMeters view provides access to data on all executions of Bit9 meters, which monitor each time a specified file is executed, in your environment. To see this information as it is displayed in the Bit9 Console, choose **Tools > Meters** in the console menu and click on the View Details button next to any meter to see information about a specific meter.

**Table 111:** ExMeters View Details

Field Name	Data Type	Special Values	Comments
Event_Id	bigint		Foreign key into ExEvents table for event that correspond to this meter entry. Since this value is always unique, it can also serve as a primary key.
Computer_Id	int		Foreign key into ExComputers table for computer that corresponds to this meter entry.
File_Catalog_Id	int		Foreign key into ExFileCatalog table for file that corresponds to this meter entry
Timestamp	datetime		Date and time when this meter entry was generated
Name	nvarchar		Name of the meter
Description	nvarchar		Description of the meter
Data	nvarchar		Data associated with the meter (see "type" for interpretation of this field)
ΔType	int	2 = sha1 hash, 3 = md5 hash, 4 = file name, 5 = sha256 hash 6 = sha256 fuzzy hash	Type of the Data field. This defines how the meter was created. <b>Change Note:</b> Some previous versions of the documentation had incorrect numerical values for this field.
User_Name	nvarchar		Name of the user that created this meter



## ExEvents

The ExEvents view provides access to all events that are displayable on the Events page. This includes events related to files discovered, files blocked, files approved, unapproved files executed, system management processes, and actions by console users. To see event data as it is displayed in the Bit9 Console, choose **Reports > Events** in console menu; this displays the Events page.

**Table 112:** ExEvents View Details

Field Name	Data Type	Special Values	Comments
<b>Event_Id</b>	<b>bigint</b>		<b>Primary Key</b>
Computer_Id	int		Foreign key into the ExComputers for computer that sent this event
File_Catalog_Id	int		Foreign key into the ExFileCatalog table for file associated with this event
Root_File_Catalog_Id	int		Foreign key into ExFileCatalog table for a root file associated with this event
▲ File_Name	nvarchar		Name of the file related to this event
▲ Path_Name	nvarchar		File path related to this event. Paths use the OS-specific delimiter for the agent on which the file is located.
Process	nvarchar		Name of the process associated with this event
▲ Process_File_Catalog_ID	int		Foreign key into ExFileCatalog table for the process associated with this event
Timestamp	datetime		Date and time (UTC) this event was generated
IP_Address	varchar		IP address of the endpoint that originated this event
Description	nvarchar		Event description
Priority	nvarchar	'Debug', 'Info', 'Notice', 'Warning', 'Error', 'Critical'	Event priority
Type	nvarchar		Event Type
Subtype	nvarchar		Event Subtype
User_Name	nvarchar		Name of the user associated with this event
▲ Rule_Name	nvarchar		Name of the Bit9 rule that caused the event (block/prompt/report/approval)

Field Name	Data Type	Special Values	Comments
◆ Ban_Name	nvarchar		Name of the hash or filename ban associated with the event (empty if the ban was not named); introduced in 7.0.1 Patch 3
◆ Updater_Name	nvarchar		If an updater is associated with the event, the name of the updater; introduced in 7.0.1 Patch 3
★ Indicator_Name	nvarchar		If a threat indicator is associated with the event, the name of the threat indicator
★ Received_Timestamp	datetime		Date and time (UTC) this event was received by the Bit9 Server
Command_Line	nvarchar		Command line for the process that attempted the action recorded by this event.

## ExFileCatalog

The ExFileCatalog view provides access to the metadata for all unique hashes of files discovered on your computers. To see this file data as it is displayed in the Bit9 Console, choose **Assets > Files** in the console menu and click on the File Catalog tab.

**Table 113:** ExFileCatalog View Details

Field Name	Data Type	Special Values	Comments
<b>File_Catalog_Id</b>	<b>int</b>		<b>Primary Key</b>
Prevalence	int		Prevalence of this file – number of computers that currently have this file
First_Created	datetime		Date and time when this file was first created
File_Size	bigint		Size of this file in bytes
File_Type	varchar	'Application', 'Package', 'Script File', 'Supporting File', 'Other', 'Unknown', 'Unrecognized Executed File'	Type of this file
MD5	char		MD5 hash of this file
Sha1	char		SHA1 hash of this file
Sha256	char		SHA256 hash of this file (see Sha256_Hash_Type for interpretation of this field)

Field Name	Data Type	Special Values	Comments
Sha256_Hash_Type	int	5 = regular hash 6 = MSI fuzzy hash	Type of the Sha256_Hash. See "SHA-256" on page 207 for more details.
First_Seen_Computer_id	int		Foreign key into ExComputers table for computer on which the file was first seen
First_Seen_Name	nvarchar		File name where this file was first seen on any computer
First_Seen_Path	nvarchar		Path where this file was first seen on any computer. Uses the path delimiter for the OS of the first-seen computer.
Product_Name	nvarchar		Product name of this file
Product_Version	nvarchar		Product version of this file
Publisher	nvarchar		Publisher of this file (if file is signed with certificate)
▲◇ Publisher_State	nvarchar	'Approved', 'Approved by Policy', 'Unapproved', 'Banned', 'Banned by Policy'	State of this publisher (if available); "none" for unsigned files <b>Change Note:</b> Banned and Banned by Policy were added during 7.0.1.
▲ Publisher_State_Reason	nvarchar	'Manual', 'Reputation', 'Imported', 'External (API)', 'Unknown'	Reason the file's publisher is approved
Publisher_or_Company	nvarchar		Publisher (if available) or Company name (if no publisher info) of this file
Company	nvarchar		Company name of this file
Installed_Program_Name	nvarchar		If this file was an installer, the name of its installed program (i.e., its name on the Add/Remove Programs page in Windows). No value for Mac or Linux files.
Trust	int	-1 = unknown, [0 – 10] valid values	Trust of this file; maximum = 10
Trust_Messages	nvarchar		More information associated with this file's trust
Threat	nvarchar	'0 - Clean', '1 - Potential risk', '2 - Malicious', 'Unknown'	Threat level of this file
Category	nvarchar		Category of this file

Field Name	Data Type	Special Values	Comments
▲ State	nvarchar	'Unapproved', 'Approved', 'Banned', 'Approved by Policy', 'Banned by Policy', 'Mixed'	Effective global file state for this file
△ File_State	nvarchar	'Unapproved', 'Approved', 'Banned', 'Approved by Policy', 'Banned by Policy', 'Mixed'	Global file state for this file <b>Change Note:</b> Was Global_State in 6.0.2. Also, values changed beginning with 7.0.0.
△ File_Flags	nvarchar	Comma-separated combination of one or more of the following: 'Installer', 'Not installer (Override)', 'Installer (Override)', 'Report Only Ban'	Global file flags for this file <b>Change Note:</b> File_Flags was Global_Flags in 6.0.2. Also, the value 'Report Only Ban' was 'Test Banned' in 6.0.2.
▲ File_State_Reason	nvarchar	'Manual', 'Trusted Directory', 'Reputation', 'Imported', 'External (API)', 'Unknown'	Reason for the approval state of this file
▲ Approved_By_Reputation	varchar	'Yes', 'No'	Was this file approved because of its file or publisher Trust and Threat ratings in Bit9 SRS
Reputation_Enabled	varchar	'Yes', 'No'	Is reputation-based approval is enabled for this file
◆ Certificate_Hash	char		Bit9-proprietary hash that provides unique identifier for this certificate.
◆ Certificate_State	nvarchar	'Unapproved', 'Approved', 'Banned', 'Approved by Policy', 'Banned by Policy'	Global State of the certificate for this file. <b>Note:</b> Invalid certificates are 'Unapproved' in this field. Unsigned certificates will be null.
◆ Certificate_State_Reason	nvarchar	'Manual', 'External (API)'	State reason of the certificate (same as Publisher State Reason)
★ File_Extension	nvarchar		Extension of first seen file with this hash

## ExFileInstances

The ExFileInstances view provides access to the metadata for each instance of each hash found on each computer at your site. To see this file data displayed in the Bit9 Console, choose **Assets > Files** in the console menu and click on the File on Computers tab. To see the complete File Instance details for any one file, from the Files on Computers tab, click on the View Details button next to the file.

**Change Note:** In Beginning with v7.0.1, the fields **Initialized** and **Top\_Level** were removed from this view and added to **ExFileInstanceGroups**.

**Table 114:** ExFileInstances View Details

Field Name	Data Type	Special Values	Comments
<b>File_Instance_Id</b>	<b>bigint</b>		<b>Primary Key</b>
File_Instance_Group_Id	int		Foreign key into ExFileInstanceGroups table for group that contains this file
File_Catalog_Id	int		Foreign key into ExFileCatalog table for details about this file
Computer_Id	int		Foreign key into ExComputers table for computer that has this file
Date_Created	datetime		Date and time (UTC) when file was created
File_Name	nvarchar		Name of this file
Path_Name	nvarchar		Path of this file. Uses OS-specific delimiter for the agent where the file is located.
Executed	varchar	'Yes', 'No'	'Yes' if this file was ever executed
Δ Local_State	nvarchar	'Unapproved', 'Approved', 'Banned'	Local state of this file <b>Change Note:</b> 'Unapproved' was 'Pending' in 6.0.2.

Field Name	Data Type	Special Values	Comments
△ Detailed_Local_State	nvarchar	'Approved (Not Persisted)', 'Unapproved (Persisted)', 'Banned by Hash', 'Locally Approved', 'Banned by Name', 'Banned by Name (Report Only)', 'Locally Approved (Auto)', 'Approved as Installer', 'Approved', 'Approved as Installer (Top Level)', 'Banned by Hash (Report Only)', 'Unapproved'	Detailed local state of this file  <b>Change Note:</b> 'Unapproved' was 'Pending' in 6.0.2. 'Unapproved (Persisted)' was 'Pending (Persisted)' in 6.0.2.
◆ Detached_Publisher	nvarchar		Name of the detached publisher. Note that embedded publishers can be retrieved through a join with ExFileCatalog.
◆ Detached_Publisher_State	nvarchar	'Approved', 'Approved by Policy', 'Unapproved', 'Banned', 'Banned by Policy'	State of the detached publisher (if available); "none" for unsigned files
◆ Detached_Publisher_State_Reason	nvarchar	'Manual', 'Imported', 'External (API)', 'Unknown'	Reason for the state of this file's publisher
Detached_Certificate_Hash	char		Bit9-proprietary hash of the detached certificate. Note that embedded certificates can be retrieved through a join with ExFileCatalog.
◆ Detached_Certificate_State	nvarchar	'Unapproved', 'Approved', 'Banned', 'Approved by Policy', 'Banned by Policy'	Global state of the detached certificate  <b>Note:</b> Invalid certificates will be 'Unapproved' in this field. Unsigned certificates will be null.
◆ Detached_Certificate_State_Reason	nvarchar	'Manual', 'Imported', 'External (API)', 'Unknown'	Reason for the state of the file's detached certificate (same as Publisher State reason)

## ExDeletedFileInstances

The ExDeletedFileInstances view provides access to the metadata for each deleted file instance on each computer at your site. The Bit9 Server keeps track of only last deleted instance of each unique file name on each computer. This means that, if same file was created and deleted multiple times, only last deleted instance will be listed.

**Change Note:** Beginning with Bit9 v7.0.1, the fields **Initialized** and **Top\_Level** were removed from this view and added to **ExFileInstanceGroups**.

**Table 115:** ExDeletedFileInstances View Details

Field Name	Data Type	Special Values	Comments
<b>Deleted_File_Instance_Id</b>	<b>bigint</b>		<b>Primary Key</b>
File_Instance_Group_Id	int		Foreign key into ExFileInstanceGroups table for group that contains this file
File_Catalog_Id	int		Foreign key into ExFileCatalog table for details about this file
Computer_Id	int		Foreign key into ExComputers table for computer that has this file
Date_Created	datetime		Date and time (UTC) when the file was created
Date_Deleted	datetime		Date and time (UTC) when file was deleted
File_Name	nvarchar		Name of this file
Path_Name	nvarchar		Path of the file. Uses the OS-specific delimiter for the agent that had the file
◆ Detached_Publisher	nvarchar		Name of the detached publisher. Embedded publishers can be retrieved through a join with ExFileCatalog.
◆ Detached_Publisher_State	nvarchar	'Approved', 'Approved by Policy', 'Unapproved', 'Banned', 'Banned by Policy'	State of the detached publisher (if available); "none" for unsigned files
◆ Detached_Publisher_State_Reason	nvarchar	'Manual', 'Reputation', 'Imported', 'External (API)', 'Unknown'	Reason for the state of this file's publisher
◆ Detached_Certificate_Hash	char		Bit9-proprietary hash of the detached certificate. Embedded certificates can be retrieved through a join with ExFileCatalog

Field Name	Data Type	Special Values	Comments
◆ Detached_Certificate_State	nvarchar	'Unapproved', 'Approved', 'Banned', 'Approved by Policy', 'Banned by Policy'	Global state of the detached certificate. <b>Note:</b> Invalid certificates are 'Unapproved' in this field. Unsigned certificates will be null.
◆ Detached_Certificate_State_Reason	nvarchar	'Manual', 'Imported', 'External (API)', 'Unknown'	Reason for the state of the file's detached certificate (same as Publisher State reason)

## ExFileInstanceGroups

The ExFileInstanceGroups view provides access to the metadata for file instance groups discovered on your computers. File instance groups are groups of files associated with one primary root file, usually their installer but in some cases a file from which they were copied.

**Table 116:** ExFileInstanceGroups

Field Name	Data Type	Special Values	Comments
<b>File_Instance_Group_Id</b>	<b>Int</b>		<b>Primary Key</b>
File_Catalog_Id	Int		Foreign key into ExFileCatalog table for details about root file of this group
Computer_Id	Int		Foreign key into ExComputers table for computer that has this file group
Date_Created	datetime		Date and time (UTC) when this file group was created
Group_Type	int	0 – initialized file 1 – top-level file 2 – file installed by process 3 – file installed by installer and can be found in add/remove programs	How the group was identified by Bit9
Path_Name	nvarchar		Path that corresponds to the root file of this group. Paths use the OS-specific delimiter for the agent on which the file is located.
User_Name	nvarchar		User that created this group
File_Name	nvarchar		File name that corresponds to the root file of this group



Field Name	Data Type	Special Values	Comments
Installed_Program_Name	nvarchar		If this file was an installer, this will be the installation name
◆ Initialized	varchar	'Yes', 'No'	'Yes' if the files in this group were found during initialization
◆ Top_Level	varchar	'Yes', 'No'	'Yes' if this group represents a top-level file that was not generated through an installer. 'No' if files in this group were part of an installation.

## ExApprovalRequests

The ExApprovalRequests view provides access to the workflow for approval requests that are created by users through the Bit9 notifier when attempts to execute a file are blocked. This includes approval requests for files that are completely blocked from running and justifications for cases in which the user responded to a prompt by allowing the file to run.

**Note:** This entire view was new beginning in v7.2.0.

**Table 117:** ExApprovalRequests

Field Name	Data Type	Special Values	Comments
<b>Approval_Request_Id</b>	<b>Int</b>		<b>Primary Key</b>
File_Catalog_Id	Int		Foreign key into ExFileCatalog table for file for which approval request was created
Process_File_Catalog_Id	Int		Foreign key into ExFileCatalog table for process associated with file for which approval request was created
Root_File_Catalog_Id	Int		Foreign key into ExFileCatalog table for root file associated with file for which approval request was created
Computer_Id	Int		Foreign key into ExComputers table for computer on which approval was requested
Date_Created	datetime		Date and time (UTC) when this approval request was created
Date_Modified	datetime		Date and time (UTC) when this approval request was last modified
Last_Modified_By	nvarchar		User that last modified this approval request
Enforcement_Level	nvarchar	Valid enforcement levels	Enforcement Level of agent when file was blocked

Field Name	Data Type	Special Values	Comments
Resolution	nvarchar	Not Resolved, Resolved - Publisher, Resolved - Installer, Resolved - Approved, Resolved - Rule Change, Resolved – Other, Rejected	Resolution of request
Request_Type	nvarchar	Approval, Justification	Type of approval request: Approval if file was blocked, Justification if file triggered a user-choice prompt
Requestor	nvarchar		User that created approval request on the agent
Requestor_Comments	nvarchar		Comments provided during approval request creation
Requestor_Email	nvarchar		Email address provided during approval request creation
Priority_Text	nvarchar	High, Low, Medium	Priority assigned to this request by the user creating it
Resolution_Comments	nvarchar		Comments provided during resolution of request
Status	nvarchar	Submitted, Closed	Current status of the request
Policy	nvarchar		Name of the Policy where agent was in when block happened
Multiple_Blocks	nvarchar	Yes, No	Whether multiple blocks happened on this endpoint and hash
File_Name	nvarchar		Name of the file that was blocked on the agent
Path_Name	nvarchar		Path of the file that was blocked on the agent
Process	nvarchar		Full path to the process that wrote the file that was blocked on the agent

## Sample Queries

The following examples show some of the types of queries you can make with the Live Inventory SDK. Note that each query must use the **das** database.

### Listing Malicious Files

If you have Bit9 SRS enabled, you can use the following query to get a listing of the file names and prevalence of all malicious files determined to be on your systems that run the Bit9 Agent:

```
USE das
SELECT First_Seen_Path, First_Seen_Name, Sha256, Threat,
       Trust, Prevalence
FROM bit9_public.ExFileCatalog
WHERE Threat IN ('2 - Malicious', '1 - Potential risk')
ORDER BY First_Seen_Path, First_Seen_Name
```

If you run this query and there is data available, you will see output similar to the following (formatting will vary):

First_Seen_Path	First_Seen_Name	Sha256	Threat	Trust	Prev.
c:\temp\folder1	myfileapp.exe	46b8d0bc3a4db843 3fb66543c1ec03bd1 e24e0198228ac702 4c0a15658bf04fd	1 - Potential risk	2	1
c:\documents and settings\rjones	numbergen.exe	552e68dcd6c2a4d6 bf9c9dbf278967e29 04cd624c23c0aad58 c430ed7fa75acd	1 - Potential risk	1	1
c:\documents and settings\bsmith	makemess.exe	4d9ab91f5e1efbc5 abcd6ec9a0a63452 35a54cf05d6241a30 4e3bf3b40d4668	1 - Potential risk	3	1
c:\hp\bin	endprocess.exe	1effc62134ab95d29 7c34959752311e1f7 f433d07810da65b23 3bf7241ada68ad	1 - Potential risk	3	13
c:\program files\mywebapp\	f4dothis.dll	abcdea797736654a e4f74eef7371d018c 3463f24cf78aea92d afe51c7a858f19	2 - Malicious	0	1
c:\jobfiles	myway.exe	23451271912da7b6 8b407c77381ab1ff3 b59b37c1e4d9f1e41 7a1d0fcc9270dd	2 - Malicious	0	1

## Listing Bit9 Agent Systems by Policy and Enforcement Level

You can use the following query to determine how many systems are running the Bit9 Agent and group the results by Policy and Enforcement Level:

```
USE das
SELECT Policy, Enforcement_Level, Disconnected_Level,
COUNT(*)
  AS Computer_Count
FROM bit9_public.ExComputers
GROUP BY Policy, Enforcement_Level, Disconnected_Level
ORDER BY Policy
```

If you run this query and there is data available, you will see output similar to the following (formatting will vary):

Policy	Connected_Enforcement_Level	Disconnected_Enforcement_Level	Count
Agent Disabled	None (Disabled)	None (Disabled)	3
Research Team	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	6
Default Policy	None (Visibility)	None (Visibility)	1
General Office	High (Block Unapproved)	High (Block Unapproved)	49
Guest Policy	High (Block Unapproved)	High (Block Unapproved)	1
IT Group	Low (Monitor Unapproved)	Low (Monitor Unapproved)	11

## Listing New Unapproved Files by Policy

You can use the following query to determine how many new unapproved files have appeared during the past 24 hours and group the results by Policy:

```
USE das
SELECT Policy, COUNT(*) FROM bit9_public.ExFileInstances fi
  JOIN bit9_public.ExComputers c
ON c.Computer_Id = fi.Computer_Id
WHERE fi.Date_Created > DATEADD(day, -1, GetUTCDate()) AND
  Local_State = 'Unapproved'
GROUP BY Policy
ORDER BY COUNT(*) DESC
```

If you run this query and there is data available, you will see output similar to the following (formatting will vary):

Policy	New Unapproved File Count
Research Team	529
General Office	101
IT Group	257

## Listing New Unapproved Files by Computer and Policy

To determine how many new unapproved files have appeared during the past 24 hours and group the results by Computer and Policy:

```
USE das
SELECT c.Computer, c.Policy, COUNT(*) as Unapproved_Count
FROM bit9_public.ExFileInstances fi
  JOIN bit9_public.ExComputers c
  ON c.Computer_Id = fi.Computer_Id
WHERE fi.Date_Created > DATEADD(day, -1, GetUTCDate()) AND
Local_State = 'Unapproved'
GROUP BY c.Computer, c.Policy
ORDER BY COUNT(*) DESC
```

If you run this query and there is data available, you will see output similar to the following (formatting will vary):

Computer Name	Policy	New Unapproved File Count
MYCORP\DESKTOP-3	Research Team	307
MYCORP\LAPTOP-1	General Office	215
MYCORP\LAPTOP-4	Research Team	32
MYCORP\DESKTOP-8	IT Group	3
MYCORP\DESKTOP-10	General Office	2
MYCORP\LAPTOP-7	General Office	1



## Appendix B

### Bit9 API

The Bit9 API is intended for programmers who want to write code to interact with Bit9 Platform, either using custom scripts or from other applications. It is a RESTful API that can be consumed over HTTPS protocol using any language that can create get URI requests and post/put JSON requests as well as interpret JSON responses.

Actions performed through the Bit9 API create an audit trail just as the same action performed from the console would. The appropriate API user taking the action is referenced in event.

There are two sections in this appendix:

- **API Authentication and Access Control** – This describes how to create an API user account and get the API Token necessary for API authentication of clients. It also describes how to configure permissions for the login accounts needed for such access.
- **Available Objects** – This is a listing and brief description of the objects you can access through the Bit9 API.

This appendix is a summary only. The full API documentation is available in two locations:

- Documentation at the time your version of Bit9 Platform was finalized is available through the Bit9 Console at <https://<serveraddress>/api/bit9platform/v1>
- The most current documentation is available at <https://github.com/carbonblack/bit9platform>. This location will include examples.

#### Note

The Bit9 Platform also includes a Live Inventory SDK, which provides read-only public views into the database. You can create your own reporting and data analysis solutions through the use of these public views. See [Appendix A, “Live Inventory SDK: Database Views,”](#) for more information.

## Overview

The current version of the Bit9 API is v1. All API calls are based at the following address:  
**https://<your server name>/api/bit9platform/v1**

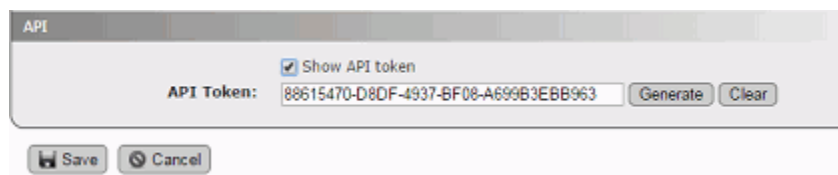
## API Authentication and Access Control

Bit9 APIs are authenticated through an API token for the login account of the currently logged in console user. This token has to be placed inside each HTTP request's 'X-Auth-Token' header.

For access control, the best practice is to have a separate console user for each API client, with the minimum required access controls. However, the API client must have access permissions similar to what would be required to access the same objects through the Bit9 Console. For example, if an API client needs to access the 'event' object, the user associated with an API token used in the client must have “View events” permission. See the full API documentation on GitHub for the permissions necessary for using each object and “[Account Group Permissions](#)” on page 93 for the steps needed to add or remove permissions. See also “[Using the Bit9 API to Add a Connector](#)” on page 686 if you intend to use the API to add a connector to the Bit9 Platform.

### To create an API user and get its API token:

1. Review the Bit9 API documentation on your server or GitHub to determine the permissions needed for your API client.
2. On the console menu, choose **Administration > Login Accounts**.
3. Click the **Groups** tab and then on the **Add Group** button. The Add Group page opens.
4. On the Add Group page, provide a Name (for example, “API Connector Extensions”), add a Description if you choose, and check the box for each permission needed for your client. Note that some permissions depend upon others, and you must have permission to view an object if you also intend to change it.
5. When you have configured the group, click the **Enabled** button in the Status line and click the **Save** button at the bottom of the page.
6. Click the **Users** tab, and on the *Login Accounts: Users* page, click **Add User**.
7. On the Add User page, provide a user name (for example, “API HashBanScript”) and password, and choose the Group you created above.
8. Provide information in any other fields you choose.
9. At the bottom of the page, check the **Show API token** box and then click the **Generate** button. A string of characters appears in the API Token box.



10. Copy the API Token to a location in which you can copy it to your API code. Also make a record of the login user name the code is associated with.
11. Click the **Save** button at the bottom of the page.



**Important**

The API Token should not be used in any way that displays it in clear text. If the API Token is compromised, open the Edit Login Account page for the API user, check the Show API token box, click **Generate** to produce a new token, and then click **Save**. Then use the new token for authentication.

To disable API access for a user that currently has permission, follow the steps above but click **Clear** instead of Generate. If server hardening is required, all API access should be removed.

**Available Objects**

You can access the following Bit9 Platform objects through the Bit9 API (see the full documentation for the actual object name in the API and to see which are read only):

- Approval Requests and Justifications – Access the workflow for approval requests and justifications created when users respond to a notifier.
- Certificates – Access publisher certificates found on endpoints and their state.
- Computers – Access computer-related properties for Bit9 Agents, change policies, upgrade agents, convert a computer to a VDI template, change debugging properties, take other advanced actions.
- Connectors – Access the configuration for network security connectors integrated with the Bit9 Platform.
- Events – Access events recorded by the Bit9 Platform.
- Files Analysis – Access files sent to network connectors for analysis; request or cancel analysis of a file.
- File Catalog – Access the record of all unique files found by Bit9 Agents, including metadata related to the files.
- File Instances – Access the live file inventory (Files on Computers) for files on all Bit9 Agents; locally approve files.
- Deleted File Instances – Access the inventory of deleted files on all Bit9 Agents.
- File Instance Groups – Access the record of file groups in the Files on Computers inventory.
- File Rules – Access rules related to unique files; create and edit Approvals and Bans.
- Files Uploaded from Agents – Access the record of files uploaded from agents to the Bit9 Server; request or cancel uploads.
- Metered Executions – Access the record of file executions tracked by a Bit9 Meter.
- Notifications – Push notifications from a network connector (services and appliances) to the Bit9 Server.
- Notifier – Access notifiers that are used when a file action is blocked because of a rule.
- Pending Analysis – Access all pending analysis requests for a given external connector.
- Policy – Access policy information.

- Publisher – Access publisher information; change publisher state (Banning or Approving).
- Server Configuration – Access configuration properties for the server.
- Server Performance – Access server performance statistics.
- Updaters – Access updater information; enable or disable updaters.

## Using the Bit9 API to Add a Connector

The Bit9 Connector allows you to integrate the Bit9 Server with one or more network security devices or services so that the external source can provide threat notifications to the server and the server can send files to the external source for detonation and/or analysis. Several connector integrations are built into the Bit9 Server and configurable through settings already in the Bit9 Console.

The Bit9 API provides a way to extend Bit9 Connector capabilities to devices and services not built into the current Bit9 Server. When correctly implemented, these connections add the notification and analysis capabilities, and the user interface elements necessary to configure and use them. The interface for configuring a new connector appears on the Connectors tab of the System Configuration page in the Bit9 Console. On this tab, you can make the following configuration choices:

- **Integration Enabled** - This checkbox enables and disables notification integration for this connector. If this box is unchecked, file analysis will also be disabled automatically.
- **File Analysis Enabled** - This checkbox enables and disables file analysis for this connector, the connector has this capability. This setting appears only if the connector allows file analysis.
- **Upload Location** -- If File Analysis is enabled, you can customize the upload location for this connector. This option appears only if the connector allows file analysis.

When configured, the new connector appears in the Bit9 Console interface wherever built-in connectors would appear. For example, if a connected device or service allows analysis, the new connector appears on the Action menu of the Files pages as an analysis option. See [Appendix C, “Bit9 Connector for Network Security Devices,”](#) for a full description of the connector capabilities and user interface.

### Notes

- To add an integration with a custom network security device or service, you must activate the “Extend connectors through API” permission for the login account that will be used for access to Bit9. Completing the configuration for a connector also requires permission to view and manage system configuration.
- Once the connector is implemented through the Bit9 API, you do not need a special license for access to its notification features. However, to upload files from a Bit9-managed computer to a third-party devices or service for analysis, you do need the separately licensed File Upload feature.

## Appendix C

## Bit9 Connector for Network Security Devices

This chapter provides instructions for configuring and using the Bit9 Connector, which integrates the Bit9 Server with one or more network security devices or services.

### Sections

Topic	Page
<a href="#">Overview</a>	688
<a href="#">Enabling Microsoft SCEP Integration</a>	689
<a href="#">Enabling Palo Alto Networks Integration</a>	692
<a href="#">Enabling Check Point Integration</a>	698
<a href="#">Enabling FireEye Integration</a>	709
<a href="#">Enabling Console Account Permissions</a>	718
<a href="#">External Notifications</a>	718
<a href="#">Banning Externally Reported Malware</a>	732
<a href="#">Analysis of Suspicious Files on Endpoints</a>	734
<a href="#">Bit9 Logging of Connector-related Events</a>	738

## Overview

The Bit9 Connector allows you to integrate the Bit9 Server with one or more network security devices or services, including:

- Check Point® Software Technologies firewalls
- Check Point ThreatCloud Emulation Service
- Check Point Threat Emulation Private Cloud Appliances
- FireEye™ Email Security and Network Security
- FireEye Forensic Analysis
- Microsoft System Center Endpoint Protection (SCEP)
- Palo Alto Networks™ firewalls
- Palo Alto Networks WildFire™ public and private cloud services

### Note

In addition to the supported devices and services, you can integrate VirusTotal and Lastline with the Bit9 Platform using the Bit9 API. These integrations are examples of API capabilities only, and not currently supported. See [Appendix B, “Bit9 API,”](#) for instructions on enabling API access and authentication, and <https://github.com/carbonblack/bit9platform> for full API documentation and access to the example code.

By integrating these systems with Bit9, when a connected device or service detects malware on an enterprise network, Bit9’s real-time endpoint sensor and recorder automatically confirms the location and scope of the threat, accelerating incident response and remediation. In addition, suspicious files found by the Bit9 endpoint sensor can be uploaded to one of the connected appliances or network security analysis providers for further analysis.

The Bit9 Connector adds the following capabilities to what the Bit9 Server and network security devices or services offer individually:

- **External Notifications** – Notifications provided by the connected sources appear as “External Notifications” in the Bit9 Console, correlated with Bit9 endpoint data to provide immediate visibility into the priority of the alert and the scope of any infection. See “[External Notifications](#)” on page 718 for details.
- **File Banning** – Malware reported by connected sources can be manually or automatically banned by Bit9. See “[Banning Externally Reported Malware](#)” on page 732 for details.
- **Registry Control** – Suspicious file or registry activity reported by connected sources can be reported or restricted by Bit9 custom rules. See “[Special Rules for Reporting or Banning Malware](#)” on page 733 for details.
- **Analysis of Suspicious Files** – Suspicious files discovered on endpoints by Bit9 Agents can be sent to connected services for analysis. See “[Analysis of Suspicious Files on Endpoints](#)” on page 734 for details.
- **Unified Event Logging** – Events related to external notification or analysis and reported to the Bit9 Server become part of the Bit9 event log, and are also available as

Syslog output. See [“Bit9 Logging of Connector-related Events”](#) on page 738 for details.

- **Event Rules** – Rules can be defined that use file-related Bit9 events to take actions. For example, a rule could send any newly discovered file in the Bit9 Server inventory to Check Point Threat Emulation Cloud Service or appliance, Palo Alto Networks WildFire cloud or FireEye AX for analysis. Another rule might be defined that automatically bans any file reported as malicious in an external notification. Or if Bit9 detects that repeated malware infections reported by Microsoft SCEP have the same parent process, an Event Rule could be created to ban that parent process if it is not used for any required function. See [“Event Rules”](#) on page 423 for a description of how Event Rules work and how to configure them.

## Preparing to use the Connector

The Bit9 Connector is a separately licensed option of the Bit9 Security Platform. To use the connector features you must do the following:

- Install the Bit9 Server with the appropriate license for Bit9 Connector, or add the license after installation.
- Configure the Bit9 Server and any of the connected devices as described in this appendix so that they can communicate with each other.
- Confirm that one or more Bit9 Console user accounts have privileges related to the Connector. Accounts in the Administrator group have these permissions by default. See [“Account Group Permissions”](#) on page 93 for details.

### Note

Contact your Bit9 representative to determine which versions of Check Point, Microsoft, Palo Alto Networks, and FireEye products are compatible with the Bit9 Connector for Network Security Devices and Bit9 Server hardware/software requirements.

## Enabling Microsoft SCEP Integration

Microsoft System Center Configuration Manager (SCCM) can be used to distribute software, manage configuration, and set security policies on endpoints and servers. One component of SCCM is System Center Endpoint Protection (SCEP), which provides anti-malware and other security features for the Microsoft platform.

You can use the Bit9 Connector to integrate with an SCCM Server so that Microsoft System Center Endpoint Protection (SCEP) notifications are sent to the Bit9 Server. These SCEP notifications may be correlated with information about files on Bit9-managed endpoints to determine where the malware is and help the security team investigate and eliminate threats. When new threats are reported, Bit9 is able to acquire a hash for the file and place it in the Bit9 inventory, even if the file is going to be quarantined.

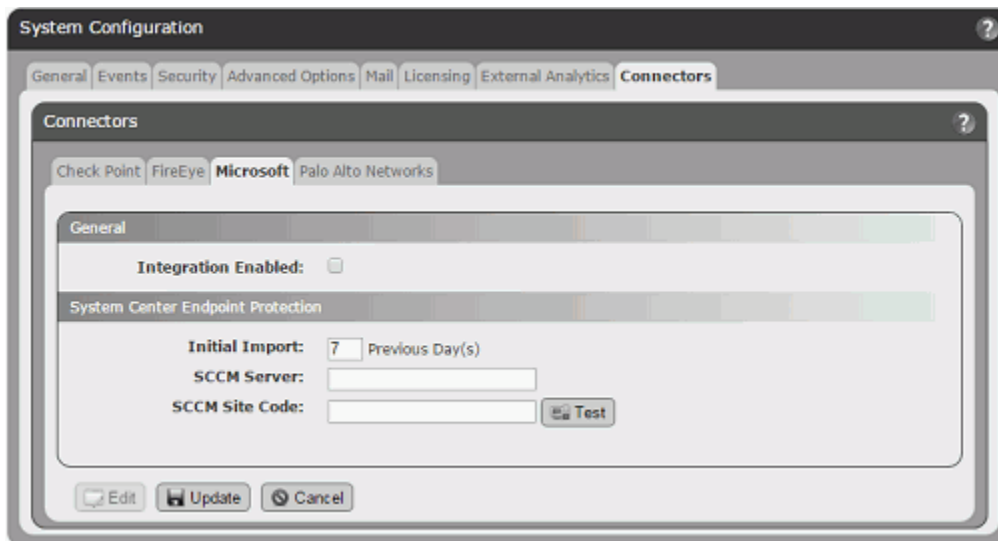
In addition to coordinating file information for threats, this integration allows the Bit9 Server to report the status of SCEP features (Anti-Spyware, Anti-Malware, and Endpoint Protection) on the Computer Details page in the Bit9 Console.

### Important

For the integration to succeed, the user running the *Bit9 Server* service must have Read-Only Analyst access rights for SCCM. This user is configured during Bit9 Server installation and can be determined by opening the Windows Task Manager and clicking the Services button in the bottom right corner.

#### To enable integration of Microsoft SCEP notifications with the Bit9 Server:

1. In the Bit9 Console, choose **Administration** > **System Configuration** and click on the **Connectors** tab and then click the **Microsoft** tab.
2. Click the **Edit** button at the bottom of the page.



3. Check the **Integration Enabled** checkbox. This is the master switch for the Microsoft SCEP integration and must be checked for any of the integration features to be activated.
4. In the Initial Import field, enter the number of days of historical notification data you want to import to Bit9. The default value is 7 days. This value affects only imports from SCCM servers that have not delivered data to the Bit9 Server yet. If Bit9 already has data from the server, data import will resume with the time of the last data received.
5. In the SCCM Server field, provide the name of the SCCM server managing Microsoft SCEP for your site.
6. In the SCCM Site Code field, enter the three-character site code used to identify this site in your Configuration Manager 2007 hierarchy.
7. When you have chosen the import initial period and provided the server address and site code, click the **Test** button to confirm that the SCCM Server and the Bit9 Server are able to communicate with each other. If the test fails, use the error message to troubleshoot the configuration.

8. If the test is successful, click the **Update** button at the bottom of the page.
9. Be sure to add the Bit9 Agent process, and its program and data directories, to the list of files not to scan with SCEP. See “[Installing Bit9 Agents](#)” on page 113 and then go to the installation instructions for specific platforms (Windows, Mac, or Linux) for a list of the specific file names and directories to exclude.

When the integration is complete, SCEP notifications begin to appear in the Bit9 Console. To see the notifications, choose **Reports > External Notifications** on the Bit9 Console menu and choose **Microsoft Notifications** on the Saved Views menu. If SCEP notifications do not appear at all, you can take the following troubleshooting steps:

- Check the Events page in the Bit9 Console for Server errors.
- Check *Bit9\Parity Server\Reporter\ParityReporter.log* for possible details of interest.
- Confirm that the user running the Bit9 Server service has Read-Only Analyst access rights for SCCM. This user is configured during Bit9 Server installation and can be determined by opening the Windows Task Manager and clicking the Services button in the bottom right corner.

See “[External Notifications](#)” on page 718 for a full description of the notification features, including the types of notifications pre-filtered from appearing in the Bit9 Console.

Once the SCCM Server is configured and integrated with the Bit9 Server, you can go to the Microsoft tab on the Connectors page to check the status of the server. A status indicator appears next to the SCCM Server field:

- A green circle indicates that there are no issues with the integration.
- A red circle indicates a problem, and in this case, an error message will appear with the indicator.
- A gray circle indicates that the integration is disabled.

For each status indicator, a tooltip provides additional information when you hover the cursor over the circle.

## SCEP Hash Identification Limitations

There are certain conditions under which Bit9 might not be able to create a hash for a new file quarantined or deleted by SCEP. This means that the file in question would not be added to the Bit9 file inventory or subject to Bit9 rules. The conditions are:

- when the Windows Explorer is used to extract a malware file from a compressed file or folder
- when a file is copied to an endpoint from a network share
- when a file identified as malware by SCEP is not one of the file types tracked as an executable or script by Bit9 (for example, if the file is a text or Word document file); in this case, you could create a Custom Rule or Script Rule to make that file type subject to Bit9 tracking, but this could have negative impacts on performance if the file type is very common

Also, while other Bit9 Connector integrations provide a hash when they send an External Notification to Bit9, SCEP does not. Normally, Bit9 Event Rules rely on a hash to allow them to trigger and take action on a file.

Bit9 attempts to associate a hash with SCEP notifications by correlating other data from the notification, such as the process name, file name, time of write, user name and

computer name. If this correlation successfully locates a hash in the Bit9 File Catalog, that hash is attached to the *Malicious/Potential Risk file detected* event after the External Notification event is processed. This can allow an Event Rule based on a *Malicious file detected* event to trigger from a SCEP notification.

#### Note

Integration with the Microsoft Security Essentials product line is not supported.

## Enabling Palo Alto Networks Integration

Enabling the Bit9 Connector for Palo Alto Networks involves configuration steps on both the Bit9 Server and the Palo Alto Networks appliance. You can enable integration for notifications, for file analysis of Bit9 files by the WildFire public or private clouds, or for both notification and analysis

### Integrating Palo Alto Networks Appliances for Notifications

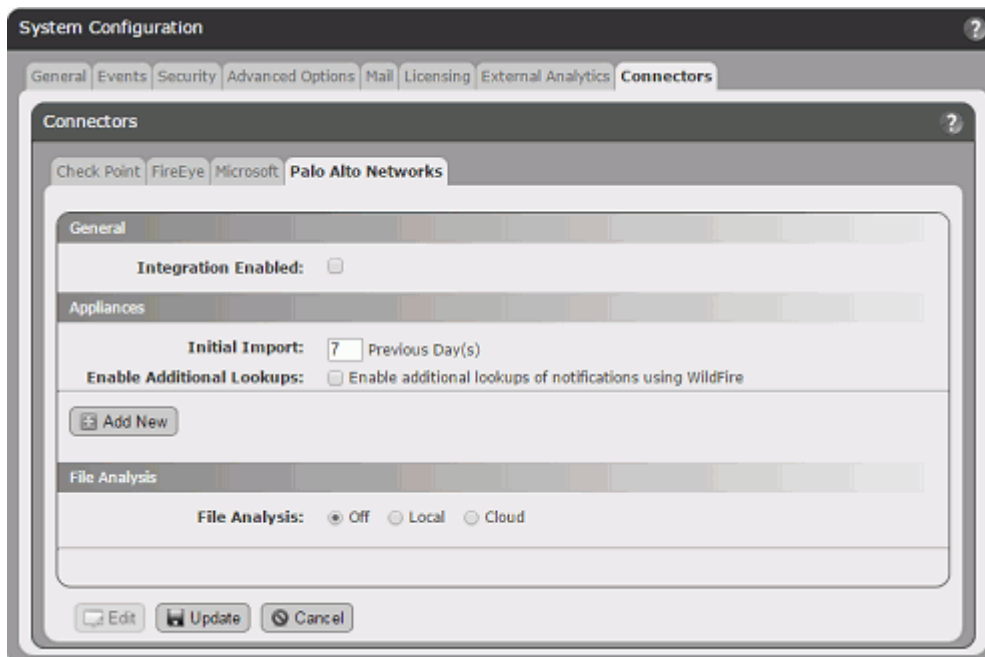
Notifications from multiple Palo Alto Networks appliances can be integrated with a Bit9 Server.

#### To enable integration of Palo Alto Networks alerts with Bit9 Server:

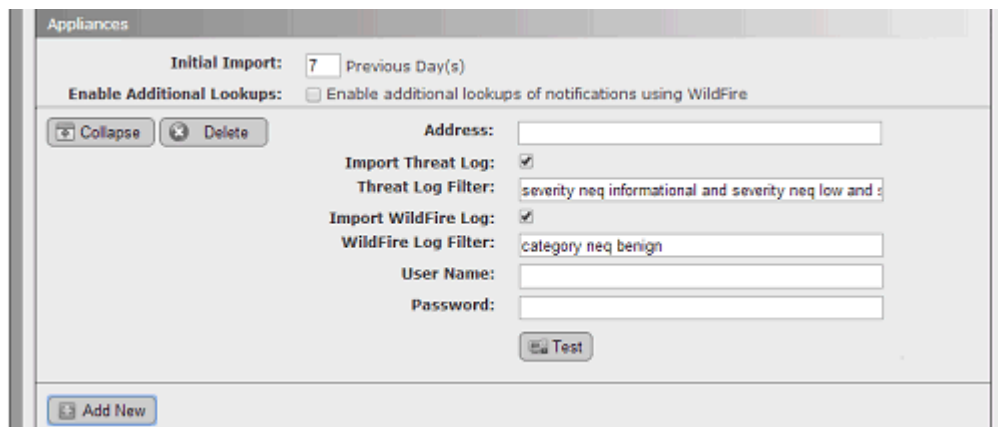
1. Confirm that the Palo Alto Networks firewall and Bit9 servers are able to contact each other.
2. On each Palo Alto Networks appliance you plan to integrate with Bit9, create a local user account with administrative read-only permissions for the Bit9 integration.
3. In the Bit9 Console, choose **Administration > System Configuration** and click on the **Connectors** tab and then the **Palo Alto Networks** tab.



- Click the **Edit** button at the bottom of the page.



- Check the **Integration Enabled** checkbox. This is the master switch for the Palo Alto Networks integration.
- In the Appliances panel, go to the Initial Import field and enter the number of days of historical notification data you want to import to Bit9. The default value is 7 days. This value affects only appliances from which no data has been received yet. If Bit9 already has data for an appliance, data import will resume with the time of the last data received.
- If you want to get a full malware report for each notification that has a file reference, check the *Enable Additional Lookups* box.  
**Important:** The Initial Import you configured will happen all at one time. If *Enable Additional Lookups* is enabled, be sure to choose an Initial Import time period that will not cause the number of WildFire cloud queries to exceed your licensed daily limit.
- The Appliances section of the Palo Alto Networks Integration Settings page allows you to add and delete appliances to the Bit9 integration.



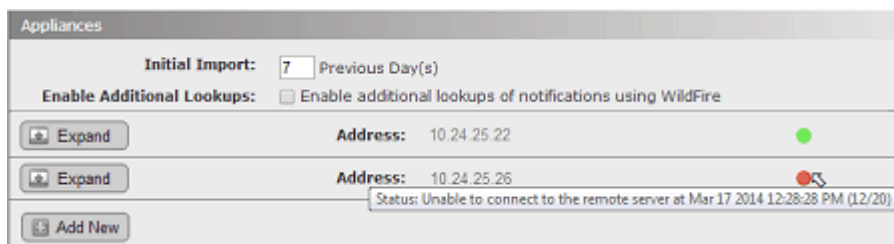
For each appliance, click **Add New** and provide the following information:

- a. **Address** – The IP address of the appliance.
  - b. **Import Threat Log** – Checking this box activates import of Threat Log data from this appliance to the External Notifications page on the Bit9 Server.
  - c. **Threat Log Filter** – This text field shows the filtering of Threat Log data from the appliance to limit what appears in the External Notifications table. By default, the filter eliminates notifications whose severity level is *informational*, *low*, or *medium*. You can modify the filter to get the notifications you choose; the filter syntax is the same as that used in the Palo Alto Networks Console.
  - d. **Import WildFire Log** – Checking this box activates import of WildFire Log data from this appliance to the External Notifications page on the Bit9 Server.
  - e. **WildFire Log Filter** – This text field shows the filtering of WildFire Log data from the appliance to limit what appears in the External Notifications table. By default, the filter eliminates notifications whose category is *benign*. You can modify the filter to get only the notifications you choose.
  - f. **User Name and Password** – In the User Name and Password boxes, enter the user name and password for the unique account you created in [Step 2](#).  
**Note:** Do not use your console login credentials for either Palo Alto Networks or Bit9 Console in these fields.
  - g. When you have provided the address and credentials, click the **Test** button to confirm that this appliance is accessible, the credentials are appropriate, and the filter syntax is valid before saving the appliance specification.
9. If you are integrating more appliances, click the **Add New** button and provide the necessary information for another appliance.
  10. The settings in the File Analysis panel determines whether files from agents managed by the Bit9 Server can be sent to the WildFire cloud for analysis. If you plan to enable WildFire file analysis, see [“Integrating with the WildFire Cloud for Analysis”](#) for information on configuring this section.
  11. When you finish configuring the integration (and if all appliances pass the Test above), click the **Update** button at the bottom of the page.

When the notifications integration is complete, Palo Alto Networks notifications begin to appear in the Bit9 Console. To see the notifications, choose **Reports > External Notifications** on the Bit9 Console menu. You might not see notifications immediately because of pre-filtering of appliance notifications. If notifications do not appear at all, check the Events page in the Bit9 Console for Server errors, and also check *Bit9\Parity Server\Reporter\ParityReporter.log* for possible details of interest.

See [“External Notifications”](#) on page 718 for a full description of the notification features, including the types of notifications pre-filtered from appearing in the Bit9 Console.

## Palo Alto Networks Notification Appliance Status in Bit9



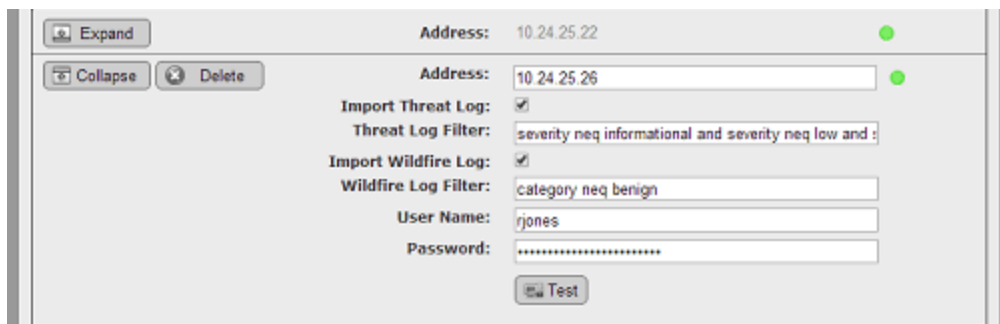
Once configured, the status of each Palo Alto Networks appliance sending notifications to Bit9 is displayed on the System Configuration/Connectors/Palo Alto Networks integration page in the Bit9 console. In the Appliances panel, a status indicator appears next to the address of each appliance:

- A green circle indicates that there are no issues with that appliance's integration
- A red circle indicates a problem, and in this case, an error message will appear with the indicator.
- A light blue circle indicates that the appliance is de-activated.

For each status indicator, a tooltip provides additional information when you hover the cursor over the circle.

## Modifying or Deleting an Appliance Integration

For any existing appliance integration, you can edit the configuration, for example, to enable or disable one or both of the Log imports to the Bit9 Server. You also can delete an appliance integration.



### To delete or edit a Palo Alto Networks appliance integration:

1. On the Connectors/Palo Alto Networks tab, click the **Edit** button at the bottom of the page.
2. Click the **Expand** button next to the appliance you want to edit. The configuration for that appliance is displayed.
3. If you want to delete an appliance from your integration, click the **Delete** button next to its address.
4. If you want to enable or disable Threat Log or WildFire log data imports to Bit9, check or uncheck the appropriate checkbox.

5. If you want to change the filter for one of the log imports, edit the text in the corresponding Filter box.
6. If you have enabled an import or modified the filter, click **Test** to confirm that the appliance is accessible and the filter syntax is valid.
7. Click **Update** to save your changes.

## Integrating with the WildFire Cloud for Analysis

You can enable uploading of files for analysis from Bit9-managed systems to either the Palo Alto Networks WildFire public cloud or a locally installed WildFire private cloud device. In either case, the file is analyzed and the analysis results are sent back to the Bit9 Console.

When the WildFire integration is complete, new menu choices appear on Bit9 Console pages that show tables of files or file details. These *Analyze with Palo Alto Networks WildFire* commands allow uploading of files to the WildFire cloud. See [“Analysis of Suspicious Files on Endpoints”](#) on page 734 for full details on how to upload files to the WildFire cloud and how to view the results of WildFire analysis.

### Note

You can connect a Bit9 Server to one or more WildFire private cloud appliances or to the WildFire public cloud, but you cannot mix private and public cloud analysis.

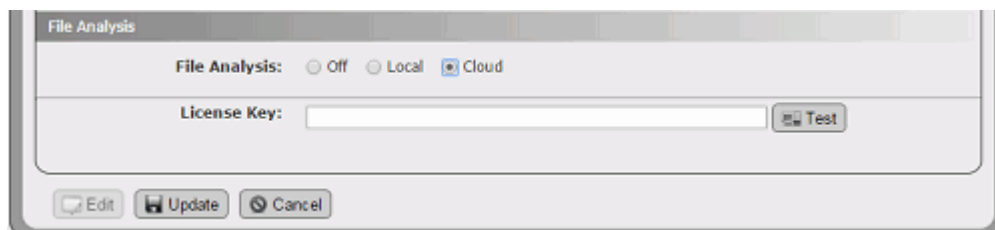
## Integrating with the WildFire Public Cloud

When you integrate the Bit9 Platform with the WildFire public cloud, the connection must be direct (not via proxy).

### To enable file uploads to the Palo Alto Networks WildFire public cloud for analysis:

1. If you are not already on this page, in the Bit9 Console, choose **Administration > System Configuration**, click the **Connectors** tab and then the **Palo Alto Networks** tab, and click the **Edit** button at the bottom of the page.
2. In the File Analysis panel, click the **Cloud** button and then enter your WildFire license key in the WildFire Key field.

**Note:** Files sent by Bit9 for analysis by the WildFire cloud service are subject to the limits in the WildFire license key.



3. Click the **Test** button next to the WildFire Key field to validate the key and the connection between the WildFire cloud and the Bit9 Server. If the test is not successful, use the failure message to troubleshoot the connection problem.

4. In the File Analysis panel, check the **File Analysis Enabled** checkbox.
5. If the WildFire Key test passed and you have finished entering the other required information, including checking the Integration Enabled box at the top of the page, click the **Update** button to save your changes.

## WildFire Public Cloud Query Limits

Enabling WildFire public cloud analysis from Bit9 will increase the number of WildFire queries per day. If the number of queries sent to the WildFire cloud per day exceeds the daily limitation, consider reducing or eliminating automated file submissions or modifying the filters determining what is submitted.

The WildFire query count is incremented by the Bit9 integration under the following circumstances:

- When Bit9 receives logs from a Palo Alto Networks appliance, the logs may reference WildFire reports. If the Enable Additional Lookups box is checked on the Palo Alto Networks Integration page, the WildFire cloud is queried for each log entry that needs to be referenced. If your query count is exceeding the limit, you may want to disable this automatic query.
- During initial import of data from the WildFire log of the Palo Alto Networks appliance after the integration is configured, a high volume of queries may occur at one time, depending on how many days you configured for Initial Import and how many WildFire log entries exist on the firewall for that period.
- When a file is submitted to the cloud from Bit9 for analysis, either manually or automatically via an Event Rule, there is one WildFire query to see if the hash for that file is already known. If it is known, it will not be uploaded and so this will be the only query. If it is not known, there will be another query to submit the file and one to query for the results of the analysis.
- If an Event Rule initiates upload of a file to the WildFire cloud but the query limit for the day has already been reached, processing of that file is delayed until the next day. This allows the license count to reset. Bit9 initiates this delay automatically, and this state is reported as tooltip if you hover the mouse cursor over the Status field of an affected file on the Analyzed Files page.

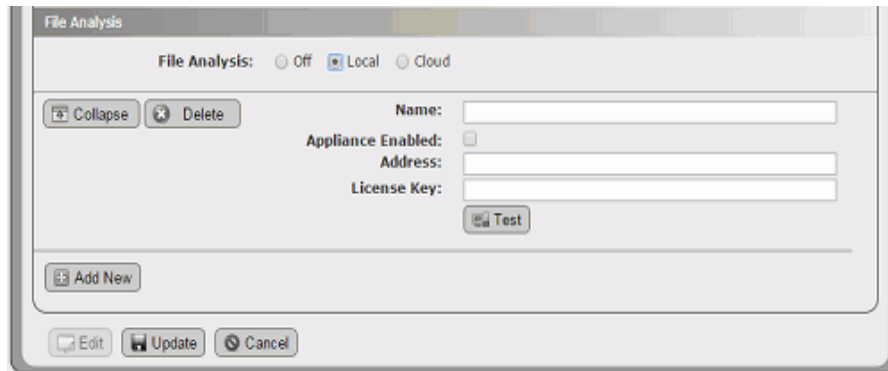
## Integrating with a WildFire Private Cloud Device

If you would rather not or cannot use a public cloud service for analysis, you can integrate the Bit9 Platform with a locally installed WildFire private cloud device. This also eliminates limits on the number of queries you can submit in any given time period. You can integrate multiple local WildFire appliances with a Bit9 Server, and analysis requests will be distributed among them.

### To enable file uploads to a Palo Alto Networks WildFire private cloud for analysis:

1. If you are not already on this page, in the Bit9 Console, choose **Administration > System Configuration**, click the **Connectors** tab and then the **Palo Alto Networks** tab, and click the **Edit** button at the bottom of the page.

2. In the File Analysis panel, click the **Local** radio button and then click the Add New button. The local appliance configuration fields are displayed.



3. In the Name field, enter the name by which you want this WildFire appliance identified in the Bit9 configuration.
4. In the Address field, enter the IP address or hostname for the WildFire appliance. Note that this should be entered as an address or name, *not* as a URL with the “https” prefix.
5. In the License Key field, enter the API key for this appliance.
6. Click the **Test** button to validate the license key and the connection between the WildFire appliance and the Bit9 Server. If the test is not successful, use the failure message to troubleshoot the connection problem.
7. In the File Analysis panel for this device, check the **Appliance Enabled** checkbox.
8. If the license and connectivity test passed and you have finished entering the other required information, including checking the Integration Enabled box at the top of the page and configuring automatic lookups if you choose, click the **Update** button to save your changes.
9. If you want to add more private cloud appliances, click the **Add New** button and repeat the configuration for another appliance.

## Enabling Check Point Integration

Enabling the Bit9 Connector for Check Point involves configuration steps on both the Bit9 Server and the Check Point cloud or appliance side. You can enable integration, configure notifications from log servers, and enable analysis of Bit9 files by either the Check Point ThreatCloud Emulation Service or by a local Private Cloud appliance. The ThreatCloud Emulation Service requires a license key.

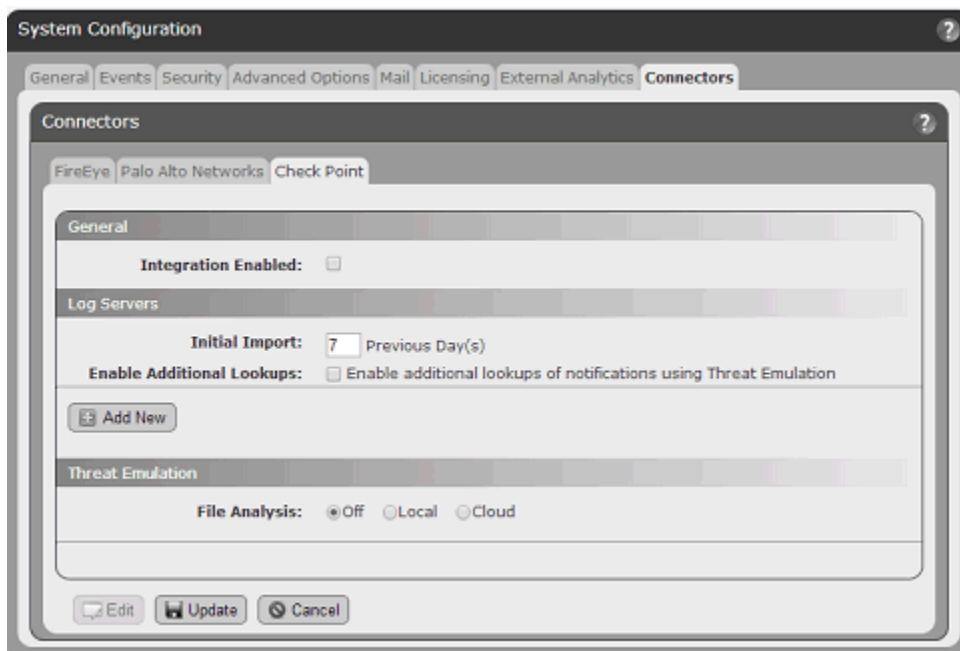
## Integrating Check Point Log Servers with Bit9

Notifications from multiple Check Point log servers can be integrated with a Bit9 Server. To perform the steps described here, you must be familiar with and have permission for advanced Check Point configuration.

### To configure integration of a Check Point log server with Bit9 Server:

1. Confirm that the Check Point log server and Bit9 server are able to contact each other, and that the port for the connection is open (by default, **18184**).
2. Make sure that the LEA server is running on the Check Point log server. If it is not, enable it.
3. Using the Check Point Dashboard, create an OPSEC application to be able to connect to Bit9 Server:
  - a. In the left lower panel click on the button for Servers and OPSEC, right click on **OPSEC Application** and choose **New OPSEC Application**.
  - b. In the Name box, enter an OPSEC Application name that clearly identifies this as an application for Bit9 connectivity; for example, **Bit9** or **Bit9\_Server**.
  - c. On the Host menu, choose the hostname for the Check Point log server you want to integrate with Bit9.
  - d. In the Client Entities panel, check the **LEA** box.
  - e. On the LEA Permissions tab, select **Show all log fields**.
  - f. Click the **Communications** button, enter the password you will use for the SSLA certificate file, record that password for later use, and click the **Initialize** button. When the initialization is complete, click the Close button on this dialog.
  - g. Click **Close** on the OPSEC Application Properties dialog. You reopen this dialog later to copy the DN field into the Bit9 configuration page for Check Point.
4. In the Bit9 Console, choose **Administration > System Configuration** and click on the **Connectors** tab and then the **Check Point** tab.

5. Click the **Edit** button at the bottom of the page.



6. Check the **Integration Enabled** checkbox. This is the master switch for the Check Point integration and must be checked for any of the integration features to be activated.
7. In the Log Servers panel, go to the Initial Import field and enter the number of days of historical notification data you want to import to Bit9. The default value is 7 days. This value affects only log servers from which no data has been received yet. If Bit9 already has data from a log server, data import will resume with the time of the last data received.
8. The Enable Additional Lookups checkbox determines the level of information received from Check Point log servers. If you want to get the full malware report for each file referenced in the threat emulation notification, check this box. Note that the lookup will occur on the ThreatCloud Emulation Service or local Threat Emulation Private Cloud appliance, depending on the configuration.

**Important:** The Initial Import you configure will happen all at one time. If *Enable Additional Lookups* is enabled during initial import, there can be a significant performance impact. Also, if you enable additional lookups, be sure to choose an Initial Import value that will not cause the number of Check Point Threat Emulation Cloud queries to exceed your licensed limit. See [“ThreatCloud Emulation Lookup Limits”](#) on page 708 for more details.



9. In the Log Servers section of the Check Point page, click **Add New** to open the configuration panel for a new server. This panel allows you to add, configure, and delete integration and connectivity between Check Point log servers and the Bit9 Server.

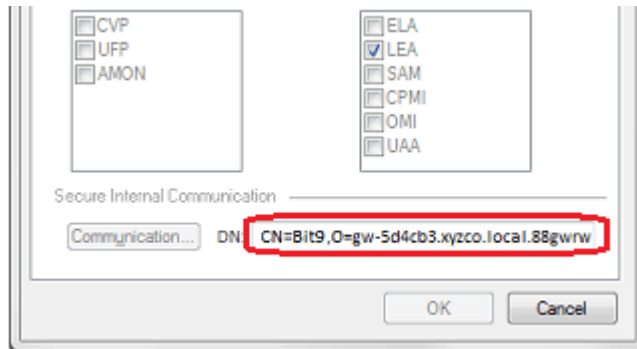
The screenshot shows the 'Log Servers' configuration window. At the top, there's a section for 'Initial Import' with a dropdown set to '7 Previous Day(s)'. Below that is 'Enable Additional Lookups' with an unchecked checkbox. The main configuration area has several fields: 'Address' (empty), 'Enabled' (unchecked), 'Port' (18184), 'Authentication Type' (SSLCA selected, None unselected), 'SIC DN' (empty), 'Password Or File' (SIC One-time Password selected, SIC Cert File unselected), and 'SIC One-Time Password' (empty). There's also an 'Import Filters' section with checkboxes for Anti-Bot, Anti-Virus, Threat Emulation (all checked), and Custom Filter (unchecked). At the bottom, there are buttons for 'Collapse', 'Delete', 'Test', and 'Add New'.

10. In the Address field, provide the IP address of the log server.
11. Check the Enabled box to enable the connection between the Bit9 Server and this log server. You may enable or disable this integration without losing the other configuration data.
12. In the Port field, enter the port to use for connecting the Bit9 Server with the Check Point log server. By default, this is **18184**.
13. The Authentication field allows you to choose secure or unsecure communication between the servers. If you want the servers to communicate in clear text, click the **None** radio button and skip to step 14.

If you want to use secure communications, click the **SSLCA** radio button (the default) and provide the following information:

- a. **SIC DN** – This Security Internal Communication (SIC) distinguished name is required for secure communication between the Bit9 Server and the Check Point log server. In the Check Point Dashboard, open the Edit dialog for the OPSEC

Application you created for Bit9. Copy the DN field from the OPSEC Application Properties dialog into the SIC DN field in the Bit9 Console.



- b. Password or File** – Radio buttons that control how the SSL certificate for the Check Point log server is downloaded to the Bit9 Server.

  - Choose **SIC One-time Password** to download a certificate file from the log server by entering the password. This choice opens an **SIC One-Time Password** box in which you enter the password you created when you created the Bit9 OPSEC Application in the Check Point Dashboard.
  - Choose **SIC Cert File** to use a previously downloaded certificate file. This choice opens an **SIC Cert File** box in which you enter the name of the certificate file. The default name for the certificate is **ops1.tmp**.
- 14.** The Import Filters section controls the data that is imported from the Check Point log servers. There are three checkbox choices corresponding to three Check Point module types: **Anti-bot**, **Anti-Virus**, and **Threat Emulation**. These are all checked by default, but you can choose to disable the import of data from any of them. There is also a Custom Filter choice, which disables the three product-specific choices and allows you to create a special filter to control data import. See [“Custom Import Filters for Check Point”](#) for a description of how to use this feature.
- 15.** When you have provided the address, credentials, certificate and filters, click the **Test** button to confirm that this log server is accessible and the filter syntax is valid before saving the configuration. If a SIC One-Time Password was provided and the certificate file was successfully downloaded, that file will be added to configuration settings.
- 16.** If you are integrating more log servers, click the **Add New** button and provide the necessary information for another log server as described in steps [10](#) through [15](#).
- 17.** The File Analysis section determines whether files from agents managed by the Bit9 Server can be sent to Check Point for analysis. If you plan to enable Check Point file analysis, see [“Integrating with Check Point for File Analysis”](#) for information on configuring this section.
- 18.** When you finish configuring the integration (and if all log servers pass the Test above), click the **Update** button at the bottom of the page.

When the notifications integration is complete, notifications from the Check Point log server begin to appear in the Bit9 Console. To see the notifications, choose **Reports > External Notifications** on the Bit9 Console menu. You might not see notifications immediately because of pre-filtering of log server notifications. If notifications do not

appear at all, check the Events page in the Bit9 Console for Server errors, and also check the following logs for possible details of interest:

- *Bit9\Parity Server\Reporter\ParityReporter.log*
- *Bit9\Integrations\CheckPoint\Bin\B9ConnectorCP.bt9*

See “[External Notifications](#)” on page 718 for a full description of the notification features, including the types of notifications pre-filtered from appearing in the Bit9 Console.

## Custom Import Filters for Check Point

There are three standard options for determining the data that is imported from Check Point log servers to Bit9: **Anti-bot**, **Anti-Virus**, and **Threat Emulation**. If you need special filters, you can choose the Custom Filter checkbox in the Import Filters field of the Connectors/Check Point tab on the System Configuration page. This disables the other filter checkboxes and opens a Custom Filter text box. All filtering is done on the log server side, reducing network traffic between the log server and Bit9 Server.

The screenshot shows the 'Log Servers' configuration window. Under the 'Import Filters' section, the 'Custom Filter' checkbox is selected. The text box contains the following filter expression: `product=Anti_Bot&severity>=2|product=New Anti_Virus&severity>=2|`. A 'Test' button is visible below the text box.

Initially, the Custom Filter box shows filters that perform the same filtering as would take place if the Anti-bot, Anti-Virus, and Threat Emulation checkboxes were checked. Examining this default custom filter can be useful in understanding the filter syntax. You add to or edit these filters or start from a blank filter window. You can resize the filter window by “dragging” the bottom right corner while holding the left mouse button down.

Filters are constructed from a Check Point log attribute, an operator, and the value you want to require for the attribute. For example:

```
severity>=medium
```

requires that a notification has a severity of at least *medium* to be imported into the External Notifications table.

Filter conditions may be combined using the AND and OR operators shown in the operators table. For example:

```
product=Threat Emulation&verdict=Malicious
```

requires that the product is *Threat Emulation* and the verdict is *Malicious*.

When you finish entering the custom filter description in the box, use the **Test** button to validate the filter syntax. A successful test validates the syntax and confirms that the Bit9 Server has connectivity with the Check Point server, but it does not indicate that any of the Check Point data would actually match the filter.

Table 118 shows the operators for filters and examples of their use.

**Table 118:** Check Point Custom Filter Operators

Operator	Description	Example
=	Equals	src=10.0.3.5
=	Attribute exists (if no parameter)	verdict=
!=	Does not equal	verdict!=benign
!=	Attribute does not exist (if no parameter)	verdict!=
>=	Greater than or equal	severity>=medium
<=	Less than or equal	severity<=low
%=	Contains string	emulated_on%=Windows 7
~=	Does not contain string	emulated_on~=Windows XP
= ,	Belongs to (used for a group)	product=Anti Virus,New Anti Virus
&	And (for combining filters)	severity>medium&verdict=benign <b>Note:</b> If AND and OR are combined, AND must always be the inner operation and OR must be the outer operation. For example: product=Anti Malware&severity>=medium  product=New Anti Virus&severity>=medium
	Or (for combining filters)	severity>medium&verdict=benign verdict=malicious

#### Note

Please note the following custom filter limitations:

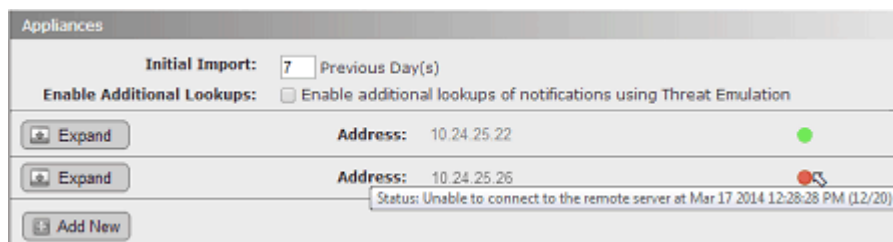
- Quotes are not supported.
- Brackets are not supported to force the operator priority or to group expressions.
- Time filtering is not supported.
- Filtering by network address may not use a network mask.

Table 119 shows some of the Check Point log attributes that can be used in custom filters. Please consult Check Point LEA field guide for the complete list.

**Table 119:** Examples of Check Point Log Attributes Used for Filters

Check Point Log Attribute (case sensitive)	Description
src	Source hostname or IP address
dst	Destination hostname or IP address
orig	Hostname of firewall generating the log entry
severity	Severity of log entry (n/a, low, medium, high, critical)
Confidence Level	Confidence level of the event
verdict	Threat emulation verdict (benign, malicious)
src_user_name	If Identity Awareness is used on Check Point, source username
product	Software product (blade) used to generate the log entry (Anti Malware, Anti Virus, New Anti Virus, Threat Emulation)
Protection name	Malware name reported by Check Point
file_type	File type (PDF, EXE etc.)
file_size	File size (in bytes)
analyzed_on	Location where the threat emulation analysis was performed (Check Point Threat Cloud or local emulation appliance hostname)

## Check Point Log Server Status in Bit9



Once configured, the status of each Check Point log server integrated with Bit9 is displayed on the *System Configuration/Connectors/Check Point* page in the Bit9 console. In the Log Servers panel, a status indicator appears next to the address of each appliance:

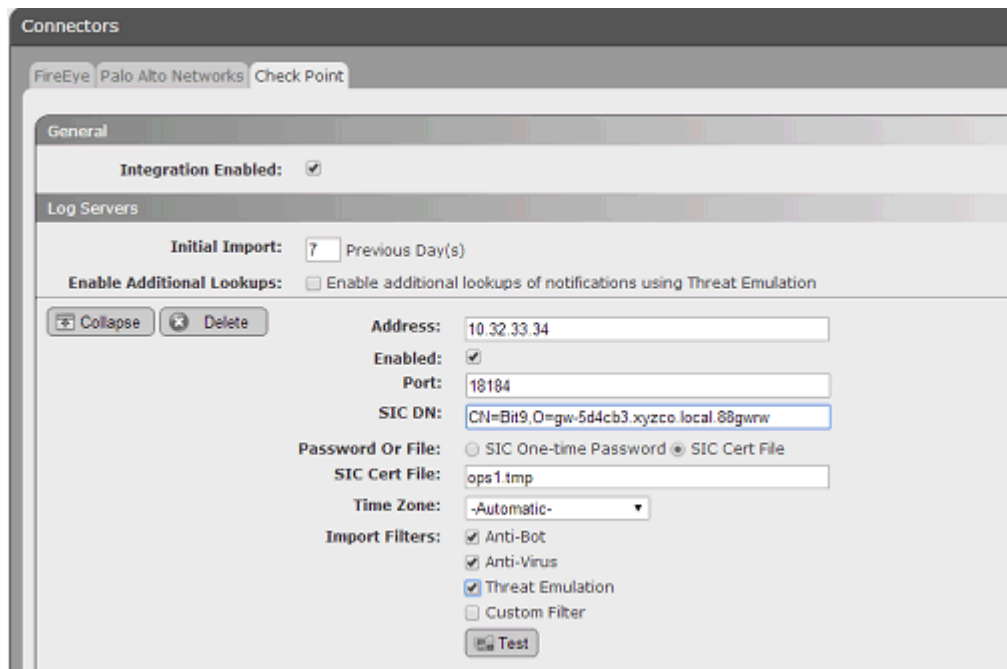
- A green circle indicates that there are no issues with that log server's integration
- A red circle indicates a problem, and in this case, an error message will appear with the indicator.
- A light blue circle indicates that the log server is de-activated.

For each status indicator, a tooltip provides additional information when you hover the cursor over the circle.

Log server connectivity errors are also shown as “Server Error” events on the Bit9 Events page and on the External Notifications page.

## Modifying or Deleting a Log Server Integration

For any existing appliance integration, you can edit the configuration, for example, to enable or disable notifications from one or more Log Servers to the Bit9 Server. You also can delete a Log Server from the integration, or disable the entire integration with Check Point.



The screenshot shows the 'Connectors' configuration page for Check Point. The 'General' section has 'Integration Enabled' checked. The 'Log Servers' section includes an 'Initial Import' of 7 Previous Day(s) and an unchecked 'Enable Additional Lookups' checkbox. A table of log servers is shown with columns for 'Collapse' and 'Delete' buttons. The configuration for a log server is displayed, including: Address (10.32.33.34), Enabled (checked), Port (18184), SIC DN (CN=Bit9,O=gw-5d4cb3.xyzco.local.88gww), Password Or File (SIC Cert File selected), SIC Cert File (ops1.tmp), Time Zone (-Automatic-), and Import Filters (Anti-Bot, Anti-Virus, Threat Emulation checked, Custom Filter unchecked). A 'Test' button is at the bottom.

### To delete or edit a Check Point log server integration:

1. On the Connectors/Check Point tab, click the **Edit** button at the bottom of the page.
2. Click the **Expand** button next to the appliance you want to edit. The configuration for that appliance is displayed.
3. If you want to delete an appliance from your integration, click the **Delete** button next to its address.
4. If you want to enable or disable log data imports to Bit9, check or uncheck the appropriate checkbox.
5. If you want to change the filter for one of the log imports, check or uncheck the standard filter boxes, or edit the text in the Custom Filter box.
6. Make any other necessary changes.
7. Click **Test** to confirm that the appliance is accessible and the filter is valid.
8. Click **Update** to save your changes.

## Integrating with Check Point for File Analysis

You can enable uploading of files from Bit9-managed systems to the Check Point Threat Emulation Service or a local threat emulation appliance for analysis and then receive the results back in the Bit9 Console. The configuration for this is in the Threat Emulation panel on the Check Point configuration page.

### Note

Bit9 correlates only data from the portion of the Check Point report entitled "unexpected activities by time", which is at the bottom of the Check Point HTML report.

## Connecting to a Threat Emulation Appliance

To enable uploading of files to a Check Point threat emulation appliance:

1. In the Bit9 Console, choose **Administration > System Configuration**, click the **Connectors** tab, and then click the **Check Point** tab.
2. Click the **Edit** button.
3. In the Threat Emulation panel, click the **Local** radio button and then click **Add New**.

4. Enter the name by which you want this Threat Emulation appliance identified in the Bit9 configuration.
5. Enter the IP address for the Threat Emulation appliance.
6. Check the box for each Analysis Environment in which you want files submitted from the Bit9 Server to be analyzed. Be sure to choose only analysis environments that are configured on the threat emulation appliance. Bit9 cannot determine programatically which environments are supported on the local threat emulation appliance.
7. Click the **Test** button to validate the address of the Threat Emulation appliance the connection between appliance and the Bit9 Server. If the test is not successful, use the failure message to troubleshoot the connection problem. One possible issue is a port mismatch. While the default for connection to the ThreatCloud Emulation Service is 18184, local appliances must use **18194**.

**Note:** The test on this page does not detect all problems with a Check Point configuration. For example, if you configure a non-existent environment, the test will not reveal that, and actions that require that environment will simply fail.

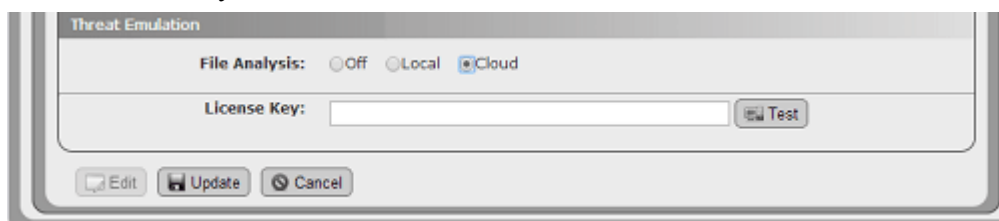
8. If the test passed and you have finished entering the other required information, click the **Update** button to save your changes.

When the analysis configuration is complete, new menu choices appear on Bit9 Console pages that show tables of files or file details. These **Analyze File with Check Point** commands allow uploading of files to Check Point. See “[Analysis of Suspicious Files on Endpoints](#)” on page 734 for full details on how to upload files to Check Point and how to view the results of Check Point analysis.

## Connecting to the ThreatCloud Emulation Service

To enable uploading of files to the Check Point cloud for analysis:

1. In the Bit9 Console, choose **Administration > System Configuration**, click the **Connectors** tab, and then click the **Check Point** tab.
2. Click the **Edit** button.
3. In the Threat Emulation panel, click the **Cloud** radio button.
4. In the Threat Emulation panel, enter your Check Point Threat Emulation Cloud Service license key.



5. Click the **Test** button next to the License Key field to validate the key and the connection between Check Point and the Bit9 Server. If the test is not successful, use the failure message to troubleshoot the connection problem.

### Note

If you need to use a proxy server for sending files from the Bit9 Server to the Check Point Threat Emulation Service for analysis, you can configure this through the Licensing tab of the System Configuration page. The Bit9 SRS Proxy Settings panel provides a field in which you can enter a proxy server address. This will be used for both Bit9 SRS and files sent to Check Point, and the proxy will be reported when you click **Test**. See “[Activating Bit9 SRS](#)” on page 643.

6. If the License Key test passed and you have finished entering the other required information, click the **Update** button to save your changes.

When the analysis configuration is complete, new menu choices appear on Bit9 Console pages that show tables of files or file details. These **Analyze File with Check Point** commands allow uploading of files to Check Point. See “[Analysis of Suspicious Files on Endpoints](#)” on page 734 for full details on how to upload files to Check Point and how to view the results of Check Point analysis.

## ThreatCloud Emulation Lookup Limits

If you add the ThreatCloud Emulation Service analysis to your Bit9-Check Point integration, be aware of the limits on the number of Check Point queries. An increase in queries will be especially noticeable if you check Enable Additional Lookups, which will



request a full report from the ThreatCloud Emulation Service on a file referenced in an external notification if the file is considered malicious and the report was not already looked up. See “[Enabling Automatic Threat Emulation Lookups](#)” for additional details.

If you find that the combined number of queries per day from your Check Point log servers appliances exceeds the lookup limits for the ThreatCloud Emulation Service, please contact Check Point for a license key extension.

## Enabling Automatic Threat Emulation Lookups

When you check Enable Additional Lookups on the Check Point configuration page, you affect both the volume of lookups and the level of detail you receive in the reports that are returned.

If you are using the ThreatCloud Emulation Service, automatic lookups count against the hourly and monthly limits specified in your license key. Enabling automatic lookups when you first enable notifications could quickly exhaust the daily limit, especially if you request input of several days previous notifications.

If you are using a local Threat Emulation appliance, there is no limit to the lookups.

The content of reports received when files are submitted for analysis varies as follows:

- **Enable Additional Lookups *disabled*** (Default) – Notifications from the Threat Emulation log contain the top-level malware file, its hash, and the file size.
- **Enable Additional Lookups *enabled*** – Notifications from the Threat Emulation log cause an automatic lookup if their Verdict is malicious and if the notification was not already looked up. The results of the lookup provide file name and registry entries and also expanded file names and registry modifications, but not file hashes or sizes for the files.

## Enabling FireEye Integration

Enabling the Bit9 Connector for FireEye involves configuration steps on both the Bit9 Server and the FireEye Console. There are two levels of integration:

- You can enable integration for *notifications only*.
- You can enable both notifications and file analysis integration.

## Performance and Bandwidth Considerations

Incoming FireEye Notifications are handled by IIS and range from 2Kb to more than 20Mb of data each. A high frequency of large notifications might impact console performance. Also, a high load from external notifications can affect the Bit9 Server and its database.

## Integrating with FireEye Notifications

**To enable integration of FireEye notifications with the Bit9 Server:**

1. Confirm that the FireEye and Bit9 servers are able to contact each other.
2. In the FireEye console, choose **Settings > Notifications**.

Notification Settings: Select a protocol type below to display and edit its parameters

	Protocol	email	http	rsyslog	snmp	Settings
Event Type	Global	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HTTP Settings Default delivery: <input type="text" value="Per event"/> Default provider: <input type="text" value="Generic"/> Default format: <input type="text" value="XML Extended"/> <input type="button" value="Apply Settings"/>
Domain Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Infection Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Malware Callback	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Malware Object	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Web Infection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

HTTP Server Listing Add HTTP Server: Name:

Remove	Name	Enabled	Server Url	Auth	Username	Password	Notification	Delivery	Account
<input type="checkbox"/>	bit9srv	<input checked="" type="checkbox"/>	https://bit9srv.m	<input checked="" type="checkbox"/>			All Events	Default	

SSL Enable:  SSL Verify:  Default Provider:  Provider Parameters:

3. On the Notification Settings page, add and configure a new HTTP listener:
  - a. Click on the **http** column header to display the HTTP Server Listing.
  - b. In the Add HTTP Server box, enter a name for the new server and click the **Add HTTP Server** button.
  - c. In the Server URL box, enter the URL for the listener file on the Bit9 Server – **https://<Bit9Server>/fireeye/listener.ashx**
  - d. On the Message Format menu, choose **XML Extended**.
  - e. Make sure the **SSL Enable** box is checked.
  - f. If authentication is required, check the **Auth** checkbox and enter the user name and password to be used. If you do not require authentication, you can leave both blank and not check the box.
 

**Note:** Do not use your console login credentials for either FireEye or the Bit9 Console in these fields. This is not a domain account. Use a unique user name and password that you also will enter on the FireEye tab of the Bit9 Console System Configuration page.
  - g. In the HTTP Settings section in the upper right, make sure the *Default delivery* setting is **Per event**.
  - h. Click the **Update** button when you have finished configuring this page.
4. In the Bit9 Console, choose **Administration > System Configuration**, click on the **Connectors** tab, and then click on the **FireEye** tab.

5. Click the **Edit** button at the bottom of the page.

6. Check the **Integration Enabled** checkbox. This is the master switch for the FireEye integration.
7. If authentication is required, enter the user name and password in the Integration Username and Integration Password boxes, respectively. If you do not require authentication, you can leave both blank.

**Note:** Do not use your console login credentials for either FireEye or the Bit9 Console in these fields. Use the unique user name and password that you entered in the Auth section of the FireEye Notification Settings in the FireEye Console.

8. Threat Level Mapping determines how the Notification Severity levels received from FireEye are mapped to Bit9 Threat Levels. There is a default mapping that maps FireEye file notifications of *any* severity to a Bit9 Threat Level of *Malicious*. You can change the mapping for the Default mapping rule, and you can add more rules so that different FireEye severities are mapped to different Bit9 threat levels. See [“FireEye Threat Level Mapping”](#) on page 715 for more information.
9. The File Analysis section determines whether files from agents managed by the Bit9 Server can be sent to a FireEye appliance for analysis. If you plan to enable file analysis through FireEye, see [“Integrating with FireEye for Analysis”](#) for information on configuring this section.
10. When you finish configuring the integration, click the **Update** button at the bottom of the page.
11. In the FireEye console, go to the **Settings > Notifications** and click **Test-Fire** on the Malware-object notification type. A notification should appear in Bit9 within a few minutes. After this validation, the FireEye integration status on the Bit9 Console System Administration/Connectors/FireEye tab page should show a green circle.

When the notifications integration is complete, FireEye notifications begin to appear in the Bit9 Console. To see the notifications, choose **Reports > External Notifications** on the console menu. If notifications do not appear, check for Server error events on the Bit9 Events page and also check the *debug.log* file in *\Bit9\Integrations\FireEye\listener* for possible errors.

See “[External Notifications](#)” for a full description of the notification features.

## Integrating with FireEye for Analysis

If you choose, you can use the notification integration alone. However, you also can enable uploading of files found on Bit9-managed systems to a FireEye appliance for analysis and receive the analysis results in the Bit9 Console.

### To enable uploading of files from Bit9 Server to a FireEye appliance for analysis:

1. Confirm that the FireEye appliance and Bit9 server are able to contact each other and that notification integration is enabled as described in the previous procedure.
2. Set up a file share for the FireEye Malware Repository as described in FireEye documentation, making sure that FireEye has appropriate access to the share. The structure under each operating system folder must be as follows:

**Table 120:** Folder Structure for FireEye Analysis

Folder Contents	Path Format	Example
Files uploaded from Bit9 for analysis	-<Ospath> - or - <Ospath>/src	d/win7sp1/ - or - d/win7sp1/src
Analysis results indicating <b>malicious</b> files	<Ospath>/bad	d/win7sp1/bad
Analysis results indicating files are <b>not malicious</b>	<Ospath>/good	d/win7sp1/good

Dashboard Analysis **Settings** Reports About

### Settings: Malware Repository

**Malware Repository Configuration**

Status: ● [ok]

Share URL:

Username:

Password:

**Configure Repositories**

Profile	Input Path	Exist	Output (Good) Path	Exist	Output (Bad) Path	Exist
win7-ap1	win7-ap1/src	●	win7-ap1/good	●	win7-ap1/bad	●
win7x64-sp1	win7x64-sp1/src	●	win7x64-sp1/good	●	win7x64-sp1/bad	●
winxp-base	winxp/src	●	winxp/good	●	winxp/bad	●
winxp-sp2	winxp-sp2/src	●	winxp-sp2/good	●	winxp-sp2/bad	●
winxp-sp3	winxp-sp3/src	●	winxp-sp3/good	●	winxp-sp3/bad	●

Poll Period:

- In the Bit9 Console, choose **Administration > System Configuration**, click the **Connectors** tab, and then click the **FireEye** tab.
- Click the **Edit** button at the bottom of the page.

**File Analysis**

File Analysis Enabled:

Appliance Name:

Appliance Enabled:

Upload Path:

Upload User Name:

Upload Password:

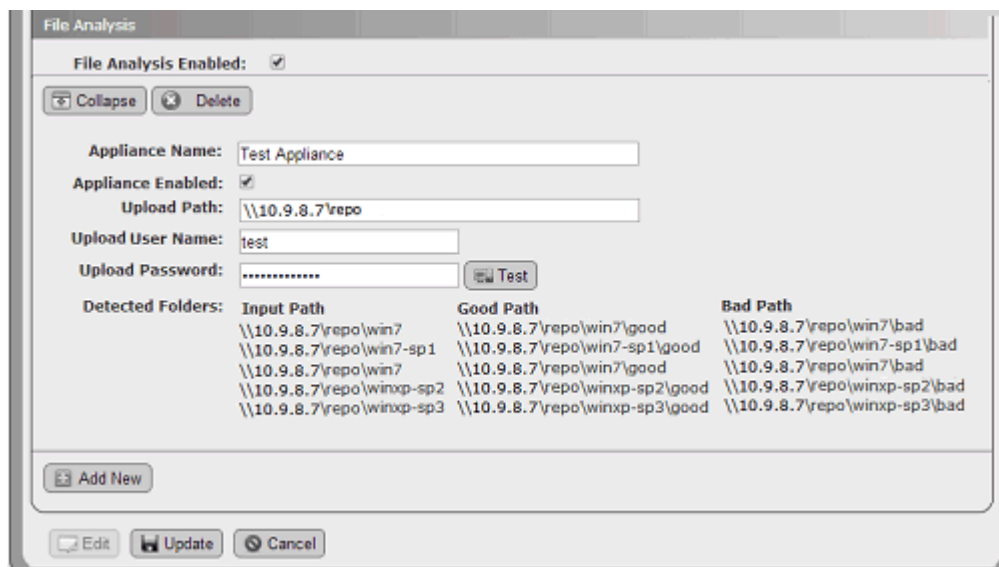
- In the File Analysis panel, check the **File Analysis Enabled** box, and then click the **Add New** button to display the fields necessary for configuring an appliance.
- Enter an Appliance Name for a FireEye appliance to which you want to be able to upload files. This name is to identify the appliance on this page only, and does not have any impact on the success or failure of the connection.
- Check the **Appliance Enabled** box to have this appliance enabled for uploads as soon as it is configured.
- In the Upload Path field, enter a path to the shared folder containing the FireEye Malware Repository.

9. Provide an Upload User Name and Upload Password for accessing the Upload Path. Consider the upload path permissions when choosing the user name to use in the Upload User Name field – this account needs read/write privileges on the upload folder.

**Note**

If you leave the Upload User Name and Upload Password fields empty, the account that installed the Bit9 Server is used as the upload user.

10. Click the **Test** button to confirm that the Bit9 Server can access the file share before updating the page with your changes. If the share is not accessible, make sure that the user account configured for the share has Read and Write permissions. If the share is accessible, the Detected Folders fields are populated with the Input, Good, and Bad Paths for each detected analysis environment.



11. When the test is successful, click the **Update** button to save your changes.
12. If you want to add more appliances, click the **Edit** button on the FireEye tab, click the **Add New** button in at the bottom of the File Analysis panel, and repeat the configuration and testing steps for the new device.

When the analysis integration is complete, new menu choices appear on Bit9 Console pages that have file or event tables, or that provide details for one file. These **Analyze File with FireEye** commands send files to the FireEye appliance. In addition, the File Analysis panel on the System Configuration page FireEye tab shows all of the operating-system-specific folders on the file share to which the Bit9 Server can delivering files. See [“Analysis of Suspicious Files on Endpoints”](#) for full details on how to upload files to FireEye and how to view the results of FireEye analysis.

**Note**

The choices on the Analyze with FireEye submenu are based on the folder structure detected when you clicked the Test button during the procedure above. If the detected folder configuration does not match the current FireEye Console share configuration, file analysis will fail when one of the unconfigured folders is chosen.

## FireEye Threat Level Mapping

Each incoming external notification causes an *External notification* event to appear in the Bit9 Server event log. If an external notification indicates malware or potential risk files, it can also generate another Bit9 event. Threat Level Mapping allows you to create one or more mappings that will generate Bit9 malware events, based on the notification that comes from a FireEye appliance. Each mapping definition can be edited, deleted and moved up or down in rank (i.e., order of evaluation).

When an external notification reaches the Bit9 Server, if it indicates malware or potential risk, it is passed through mappings that determine how it generates Bit9 events. These mappings look at fields specific to external notifications, such as severity and type, and allow you to limit event generation to a subset of notifications. The mappings are processed in order, top to bottom. The first mapping that matches the notification and has an Assign Threat Level value other than None generates the event and stops the evaluation of other mappings.

The subtype of the event generated in the Bit9 Console will depend on the Assign Threat Level value:

- If Assign Threat Level is set to “Malicious”, matching notifications generate a *Malicious file detected* event.
- If Assign Threat Level is set to “Potential risk”, matching notifications generate a *Potential risk file detected* event.

Only one threat level event can be generated per notification. If no mappings match the notification, there will only be the “External notification” event, without a related threat level event.

Bit9 malware events generated from external notifications provide the following:

- an audit trail for malware activity (see “[Bit9 Logging of Connector-related Events](#)” on page 738)
- a trigger for Event Rules, allowing you to automatically generate file bans ([Chapter 16, “Event Rules”](#))
- a trigger for a Bit9 Malicious File Alert or Potential Risk File Alert, which can also send an email notification if so configured (see “[Using Bit9 Alerts](#)” on page 494)

**Note**

You can use Threat Level Mapping to not just control malware event generation but also to eliminate the initial external notification for uninteresting data. See “[Limiting Notifications to Mapped Threats](#)” on page 717.



## Default Threat Level Mapping Rule

Initially, there is only one pre-defined mapping that covers the most general use case in which you want *any* malware-related notification to generate a malicious file event in the Bit9 event log. The following shows the settings for this mapping:

Threat Level Mapping

Import Only Mapped Notifications:

Mapping Name:

Minimum Notification Severity:

Include Notification Type:  All Types  Selected Types

Assign Threat Level To:  Top Level File Only  All New and Modified Files

Assign Threat Level:

## Adding or Editing Threat Level Mappings

Each threat level mapping must have a unique name. *Malicious file detected* and *Potential risk file detected* events generated because of a mapping include the mapping name as the Rule Name in their listing on the Bit9 Events page as shown below.

Rule Name	Description
Mark All Top Level Notifications as Malicious	File 'af.tmp' [C40F9...770A0] was identified by Parity Knowledge as a malicious file.
Mark All Top Level Notifications as Malicious	Unknown file 'lware 3.exe' [C4A89...8AC86] was identified by FireEye as malicious.
Mark All Top Level Notifications as Malicious	Unknown file 'lware 3.exe' [C4A89...8AC86] was identified by FireEye as malicious.
Mark All Top Level Notifications as Malicious	File "" [D41D8...8427E] was identified by FireEye as malicious.
Default	File 'ctime.exe' [B6988...BA771] was identified by Palo Alto Networks as malicious.

### To create a new threat level mapping:

1. On the Bit9 Console menu, choose **Administration > System Configuration**, click on the **Connectors** tab, and then click on the **FireEye** tab.
2. Click the **Edit** button at the bottom of the page.
3. In the Threat Level Mapping panel, click the **Add New** button. A new mapping definition section appears in the Threat Level Mapping panel.
4. Provide a unique name for the new rule in the Mapping Name field.
5. Choose the Minimum Notification Severity of the incoming notification. Notifications at this severity or greater will be mapped. Lower severities will be ignored by this mapping. The choices (in descending severity) are: **Critical, Major, Minor, and Any**.
6. In the Include Notification Type field, choose which types of notifications you want to match this mapping. You can choose **All Types** or **Selected Types**. For selected types, you can include one or more of the following: **Malware Object, Malware Callback, Web Infection, Infection Match, or Domain Match**.
7. You can choose to assign the threat level from this mapping to either the **Top Level File Only** or to **All New and Modified Files** associated with the notification (i.e., the malware itself and files it has created).



8. The final parameter, Assign Threat Level, determines the Bit9 event subtype that is generated when a notification matches this mapping. The choices are **None**, which does not generate an event, **Potential risk**, and **Malicious**.
9. If you want to change the order of this mapping so that it is processed before or after other mappings, use the up or down arrows to move it. Mappings are processed in the order they appear on the page, and only the first matching mapping is processed.
10. When you have completed the definition, click the **Update** button at the bottom of the page. A confirmation dialog allows you to save or dismiss your changes.

You can edit an existing mapping, changing any of its parameters and moving it up or down relative to other rules.

#### To edit a threat level mapping:

1. Click the **Edit** button on the FireEye tab of the System Configuration page.
2. If you only want to change the order of the mapping, use the up or down arrow next to the mapping name and click the **Update** button when you have repositioned it.
3. To make other changes, click the **Expand** button next to the mapping you want to edit.
4. Edit the parameters as described in the procedure for creating a new mapping, then click **Update** and confirm your changes in the dialog.

## Limiting Notifications to Mapped Threats

You can configure the Bit9 Server to accept only those notifications that match one of your mapping rules. This reduces the number of External Notifications collected on the server and the events that correspond to these notifications, making it easier to concentrate on the notifications you are interested in. Be sure that you examine your mapping rules to see what notifications will be eliminated before activating this feature.

#### To filter out non-mapped FireEye notifications:

- On the FireEye configuration page, click **Edit**, check the **Import Only Mapped Notifications** box in the Threat Level Mapping panel, and click the **Update** button.

## FireEye Appliance Status in Bit9

Once configured, the status of the FireEye integration with Bit9 is displayed in the General panel of the System Configuration/Connectors/FireEye Integration Settings page in the Bit9 console. A status indicator appears next to the address of each appliance:

- A green circle indicates that there are no issues with that appliance's integration, and is accompanied by a timestamp for the most recent notification.
- A red circle indicates a problem, and an error message will appear with the indicator.
- A light blue circle indicates that the configuration has been updated and Bit9 is waiting for the next FireEye notification.

## Enabling Console Account Permissions

To use the Bit9 Connector features, a Bit9 Console user must have certain permissions enabled in their user account. In addition to general administrative privileges for access to

the configuration pages, the list below shows permissions specifically needed for access to Connector features. Full descriptions of these permissions and instructions on how to add them to a console user’s account are described in “Account Group Permissions” on page 93.

- Tools: View file uploads (enabled by default for Administrator accounts)
- Tools: Submit files for analysis (enabled by default for Administrator accounts)

## External Notifications

Enabling the Bit9 Connector adds an External Notifications page to the Bit9 Console. This page is a table of notifications from network security devices and services. Each row in the table includes key information such as file hashes and source IP addresses. If the file or computer in a notification is also in Bit9 endpoint data, that data can be correlated with the notification.

In addition to notifications, this page will show an error message if there is a problem receiving notifications from any of the configured connected devices or services.

Notifications from Palo Alto Networks are pre-filtered to eliminate those not likely to be of interest for security analysis purposes. If a Threat Log notification has a Severity equal to “informational”, “low”, or “medium”, by default it is not included in the notifications delivered to the Bit9 Server. Also, WildFire Log notifications with a Category of “benign” are filtered out by default. Check Point notifications are also pre-filtered.

A daily check is done on the total number of notifications from all sources. If the daily check finds that this number is excessive, the oldest notifications in the logs are trimmed. Note, however, that the number of notifications may exceed the limit by a considerable amount before trimming is scheduled, such as when notifications are first enabled.

In addition to trimming notifications after they reach a numeric limit, the server deletes notifications past a maximum age. Initially, the numeric limit is 200,000 notifications and the age limit is six months. These may be modified in the future.

### To open the External Notifications table in the Bit9 Console:

- Choose **Reports > External Notifications** on the Bit9 Console menu.

Action	Time	Bit9 Status	Vendor	Severity	Type	Source Address
<input type="checkbox"/>	Mar 21 2014 12:29:38 AM	Notified	Palo Alto Networks	high	vulnerability	abc-123.de.mynet.net
<input type="checkbox"/>	Mar 20 2014 01:24:59 PM	Notified	Palo Alto Networks	critical	vulnerability	rjones.xyzco.local
<input type="checkbox"/>	Mar 20 2014 10:05:27 AM	Notified	Check Point	3	threat emulation	10.11.16.11
<input type="checkbox"/>	Mar 19 2014 05:42:00 PM	Notified	Check Point	4	threat emulation	10.11.16.11
<input type="checkbox"/>	Mar 19 2014 05:41:59 PM	Notified	Check Point	4	threat emulation	10.11.16.11
<input type="checkbox"/>	Mar 19 2014 01:03:25 PM	Notified	FireEye	major	malware-object	

Because of the data correlation with the Bit9 Server, external notifications can be prioritized immediately by their impact on systems running Bit9 Agents. When a malware notification is received from a connected network security source, you can determine:

- Whether the malware is present on any of your systems
- Whether it has ever executed on any of the systems
- How much it has spread (i.e., on how many computers)
- Details on the system identified as the source for this malware, including what kind of user activity there was on the system and other system activity

The External Notifications table includes several ways to drill down for additional information:

- The View Details (file and pencil) button opens the External Notification Details page for the notification in its row. The details page includes all of the information stored in your Bit9 database for this notification. See [“External Notification Details”](#) on page 725 for more information. It also includes a link to open the full XML details file for the notification. See [“Showing XML Details”](#) for more information on this page.
- If there is a number greater than zero in the Total Files or New and Modified Files column, clicking on the number also opens the External Notification Details page.
- If the Malware MD5, SHA-1 or SHA-256 hash is listed in the table and identifies a file inventoried by your Bit9 Server, clicking on the hash opens the File Details page for that file.
- In any of the Bit9 Files columns, if the number of files shown is 1, clicking on the number opens the File Details page for that file. If it is 2 or greater, clicking on the number opens the External Notification Details page with the Known Files tab showing.
- In the Bit9 Computers column, if the number of computers shown is 1, clicking on the number opens the Computer Details page for that computer. If it is 2 or greater, clicking on the number opens the Computers table.
- If the Source or Destination Address column shows an address for a system that has the Bit9 Agent installed, clicking on the address opens the Computer Details page for that computer.
- The History button opens the Notification Details page with the History tab showing. The History tab includes the 20 most recent actions related to this notification.

[Table 121](#) shows the information available in the External Notifications table. Not all of these columns appear in the table by default.

**Table 121:** External Notifications Table Columns

Column	Description
Vendor	Vendor whose product sent the external notification. Currently Check Point, FireEye or Palo Alto Networks
Appliance	Name of the external appliance or service that provided the notification; has link to appliance or service console URL. For Check Point, if the notification came from a private threat emulator, its name is shown here.

Column	Description
Product	External appliance or service product name, if provided; has link to appliance console URL.
Version	External appliance, agent, or report version; has link to appliance console URL.
Time	Date and time when the malware was detected on the network.
Severity	Severity of notification. Scale varies by vendor.
Type	Type of notification (not the name). <b>For Check Point</b> this can be any of the configured Check Point software products (blades) that can deliver a notification. <b>For FireEye</b> this can be: domain-match, malware-callback, malware-object, web-infection, infection match <b>For Microsoft SCEP</b> this can be a string that begins with the prefix "malware_" or "potential_risk_" and ends with the object being reported by the SCEP file path header; examples include "potential_risk_file" and "malware_webscript" <b>For Palo Alto Networks</b> this can be: wildfire, spyware, virus, vulnerability, wildfire-result
Source IP	The IP address from which the malware originated.
Source Address	Source Address is the address from which the malware originated, from one of the following sources: <ul style="list-style-type: none"> <li>• If the address is for a computer known to your Bit9 Server, the hostname listed for this source in the Bit9 database is used. In this case, the name is linked to the Computer Details page.</li> <li>• If the computer is unknown to your server, the server performs a reverse DNS lookup, and if the hostname can be resolved in this way, it will be used here and will persist.</li> <li>• If Bit9 cannot resolve the hostname, a URL is shown, as resolved by the provider</li> <li>• If no resolution is possible, an IP address is shown. This would be the case if malware was attempting a callback.</li> </ul>
Source URL	URL of the computer on which the malware was originated, as resolved by the provider.
Source Username	Name of user logged into the system at the Source Address. Appears for Check Point, Microsoft and Palo Alto Networks integrations if Active Directory is integrated with the appliance or service.
Destination IP	IP address to which the malware was targeted.
Destination Address	Address to which the malware was targeted, resolved as described for Source Address.
Destination Username	Name of user logged into the system at the Destination Address. Appears for Check Point and Palo Alto Networks integrations if Active Directory is integrated with the appliance or service.
Malicious	Shows whether the notification identifies malicious files (Yes/No).

Column	Description
Malware Name	Malware name reported in notification (can be multiple, comma separated). For FireEye and Microsoft SCEP, linked to their external site with malware name descriptions.
Malware MD5	Top-level MD5 hash reported in notification.
Malware SHA1	Top-level SHA1 hash reported in notification. Appears for Check Point and Microsoft notifications.
Malware File	Top-level filename reported in notification.
Application	Application reported in the notification.
Analysis Environment	Operating System environment used for file analysis. For Palo Alto Networks and Check Point, may also include information about key applications in the environment, such as Office.
Registry Keys	Number of registry key modifications reported in the notification.
Directories	Number of directory modifications reported in the notification.
New and Modified Files	Number of files created or modified by this malware as reported in this notification.
Total Files	Total number of unique files in this notification.
Received Time	Date and time this notification was received by the Bit9 Server.
Modified Time	Date and time when this notification was last modified (i.e., its status changed).
Bit9 Status	Status of the notification in Bit9 (Notified, Escalated, Resolved, Closed).
Bit9 Known Files	Number of unique files in this notification known to the Bit9 Server. May change based on the Correlate with Bit9 option on the External Notifications page.
Bit9 Executed Files	Number of files in this notification known to the Bit9 Server and executed on an endpoint. May change based on the Correlate with Bit9 option on the External Notifications page.
Bit9 Banned Files	Number of files in this notification known to the Bit9 Server and banned. May change based on the Correlate with Bit9 option on the External Notifications page.
Bit9 Computers	Number of Bit9-managed computers that have at least one file matching one of the reported MD5 hashes in this notification.
Bit9 Files On Computers	Total number of instances on Bit9-managed computers of files reported in this notification.
Bit9 Submitted	Indicates whether a file from this notification was submitted to an external device by this Bit9 Server for file analysis (Yes/No).

## Action Menu on External Notifications Table Page

The Action menu on the External Notifications page includes the commands for changing the status of one or more notifications checked in the table and for retrieving more information about files referenced in them. Note that the notification management

commands are strictly for convenience in managing them and have no impact on files in the notifications:

- **Escalate Notification** – This indicates that the notifications are of interest and you intend to investigate and/or take action related to them.
- **Resolve Notification** – This indicates that you have finished responding to these notifications.
- **Close Notification** – This indicates that you have resolved these notifications, made any necessary comments on the External Notification Details page, and no longer need to track them.
- **View Bit9 SRS Cloud Data** – If Bit9 SRS is activated and an MD5 hash is included in the notification, opens the Bit9 SRS website and displays any information available for these hashes in the checked notifications.

## Saved Views on the Notifications Table Page

By default, the External Notifications page shows all notifications that have come to the Bit9 Server from a network security device. The pre-configured Saved Views may help focus the view on certain types of notifications:

- **Active Notifications** – Shows all notifications that do not have a status of Closed and were not a result of an analysis request from the Bit9 Console. See [“Managing Notification Status”](#) for a discussion of notification status. This is the default view.
- **Check Point Notifications** – Shows all notifications received from Check Point log servers.
- **File Analysis Results** – Shows all notifications from files that were submitted for analysis from the Bit9 Console.
- **FireEye Notifications** – Shows the notifications received from FireEye devices that were not for files submitted from the Bit9 Console.
- **Microsoft Notifications** – Shows the notifications received from Microsoft SCEP.
- **Notifications with Files** – Shows any notifications that include at least one file hash, whether or not that file is known to the Bit9 Server.
- **Notifications with Files on Bit9 Computers** – Shows any notifications that include at least one file hash for a file known to the Bit9 Server because it is or was on an agent-managed system.
- **Palo Alto Networks Notifications** – Shows the notifications received from Palo Alto Networks devices.

As with other Bit9 Console table pages, you can customize the view using the Show Filters and Show Columns buttons, and you can save any customized view you choose.

## Notification Table Access from File Details Pages

On the File Details and File Instance Details pages, if there are any notifications from network security devices for the current file, an **External Notifications** choice appears on the Related Views menu. Clicking on this link opens the External Notifications table page filtered to show only notifications that include this file.

## Choosing Correlation Level for External Notifications

A key feature of the Bit9 Connector is the correlation of security notifications received from external sources with the real-time file data available for Bit9-managed computers. In addition to the normal filtering and table column choices available for all Bit9 tables, the External Notifications page includes a menu that allows you to choose which files you would like correlated with notification data.

The *Correlate with Bit9* panel includes the following choices:

- **New and Modified Files** – This choice correlates Bit9 information with all files reported in the notification, including the top-level malware and any files it writes or modifies.
- **Only Untrusted Files** – This choice correlates Bit9 information only for files in the notification for which the trust level reported by Bit9 SRS is **5** or less.
- **Only Top Level Files** – This choice correlated Bit9 information only for top-level files reported in the notification, not files written or modified by these files.
- **Include Deleted Files** – This is a checkbox that is applied to any of the menu choices. If checked, files deleted from Bit9 endpoints are included in those correlated with notification data. This can be a good choice when you want to be sure to track malware that deletes itself after execution, which is very often the case.

### Note

You also can change the Correlate with Bit9 choice on the Known Files and Files on Computer tab within an External Notification Details page. A change in any of these locations affects all notification tables.

MD5 hashes included in external notifications are used to correlate with files in the Bit9 Server inventory. If a notification does not include an MD5 hash but does provide a SHA-256 hash, the SHA-256 hash is used for correlation.

In a small number of cases, Bit9 creates a "fuzzy" hash in its file inventory for files that change their hash every time they are installed because they include date, location, or other context-specific information. These hashes are identified as "SHA-256 (Normalized)", and they may not be able to correlate with SHA-256 hashes reported in external notifications. This is relevant only if there is no MD5 hash in the notification and the file identified in the notification required a fuzzy SHA-256 hash in the Bit9 Server's file inventory.

For both the malware file and its parent process, file correlation begins immediately upon receipt of the notification by the Bit9 Server and continues as a background task for as long as is necessary to process the notification and synchronize with Bit9 file inventory processing. This is repeated for all unknown files until they are successfully correlated or until the notification is considered obsolete, normally 24 hours. This time period allows for correlation of a large number of new files whose notifications may arrive at the Bit9 Server before the server has processed the file into the Files on Computers inventory.

When files are successfully correlated, a Malicious file detected or Potential risk file detected event is generated containing the hashes of both the malware file and its parent process. If there are multiple files in the notification, the event is generated only for the

top-level file. In the notification table and details, these hashes are links to Bit9 File Details page for the respective files.

### Note

When a file keeps the same name but it changes and its hash changes, correlation can be attempted with the new hash, but if the new hash does not appear in a notification, the correlation will fail.

## Notifications from Multiple Analysis Environments

Action	Time	Vendor	Analysis Environment	Malware File
<input type="checkbox"/>	Nov 25 2013 04:15:06PM	Palo Alto Networks	Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007	TEST-FILE.EXE
<input type="checkbox"/>	Nov 25 2013 04:15:06PM	Palo Alto Networks	Windows 7, Adobe Reader 11, Flash 11, Office 2010	TEST-FILE.EXE
<input type="checkbox"/>	Nov 25 2013 03:54:47PM	Palo Alto Networks	Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007	TEST4.DOC

Check Point and WildFire (6.0 and later) can report multiple notifications for the same file, each from a different analysis environment. The Analysis Environment field is especially useful in this case since it provides information about the test environment(s) in which the file was detonated or analyzed, allowing you to determine whether or not the file was found malicious in each environment. For notifications based on detonation of a file, the environment includes not only the base operating system but also other key software. For example, one notification might show the following Analysis Environment: *Windows 7, Adobe Reader 11, Flash 11, Office 2010*

For WildFire notifications that involved static analysis, the type of analyzer is reported in this field, for example: *DOC/CDF Analyzer*.

### Note

If a file is uploaded from Bit9 to the WildFire cloud for analysis and WildFire reports multiple notifications for the file, the file might be considered benign in some environments and malicious in others. The External Notifications table and External Notification Details pages show the individual analysis results for each Analysis Environment. However, for a file submitted to the WildFire cloud, the Analyzed Files tab of the Requested Files page shows only the combined overall results for the file as determined by WildFire.

## External Notification Details

The External Notification details page includes all of the information stored in your Bit9 database for one notification.

**To open the External Notification Details page for one notification:**

1. Choose **Reports > External Notifications** on the Bit9 Console menu.



- In the row for the notification of interest, click the View Details button.

The Details page includes basic information about the notification plus a series of tabs with more details at the bottom of the page. The tabs vary depending upon what type of notification it is. Most of the fields on both the main page and the tabs are described in [Table 121](#) on page 720. Information about the tabs is provided in the following sections.

## Total Files Tab

This tab shows all of the files reported in this notification, including files written by other files. If the same file (i.e., a file with the same hash) is written to multiple locations, it appears multiple times in the Total Files list. The table includes the following columns:

**Table 122:** Total Files Tab Columns

Column	Description
Sequence	Sequence of each file's appearance when a suspected malware instance is analyzed by the network security device. The first file in the sequence is the top-level process.
Operation	The operation performed on a file (start, create, close, etc.) For Microsoft SCEP notifications, this is always "create".
File Name	File name reported by the network security device. For Check Point, only reported for the first file.

Column	Description
Size	File size reported by the network security device. For Check Point, only reported for the first file.
MD5	MD5 hash of the file. For Check Point, only reported for the first file.
File Path	File path of the file name reported in the notification.
Parent File Name	File name of the parent process of this file.
Parent File Path	File path for the parent process of this file.
SHA1	SHA1 hash of the file (if reported). For Check Point, only reported for the first file.
SHA-256	SHA-256 hash of the file (if reported). Only shown for Palo Alto Networks notifications.
Known File	Is this file known to the Bit9 Server (Yes/No).

The Operation column provides important information about what was done for each file included in the notification. You can sort or filter on this field to determine what was done to a file. The notification might report that one file was *created* and another *overwritten* – files having these two operations are included in the New and Modified Files list. A file also might be *opened* or *terminated*.

If a file is known to your Bit9 Server, its listing on the Total Files tab includes a View Details button, which opens the File Details page for the file.

The Action menu for this tab includes the following commands for selected files:

- **Ban Globally** – Bans file(s) for all policies; requires no further configuration
- **Ban By Policy** – Opens a dialog box for creation of policy-specific and report-only bans
- **Remove Approval Or Ban** – Removes any active bans/approvals immediately.
- **Find By Name** – Redirects to Find files page filtered by selected file names
- **Find By Size** – Redirects to Find files page filtered to show results of a search for files matching the sizes of the selected files as reported in the external notification
- **Find By Hash** – Redirects to Find files page filtered to show results of a search by hash for the selected files as reported in the external notification
- **View Bit9 SRS Cloud Data** – Redirects to Bit9 SRS for report on this file by hash (if SRS is activated)

## Known Files Tab

This tab shows all files from this notification that are known to the Bit9 Server. The table includes (either by default or customization) all fields from the Bit9 File Catalog. You also can add other fields that provide information about the file from the network security device, as shown on the Total Files tab. The Action menu has the same options as the Total Files tab menu, but uses file information from the Bit9 inventory rather than the notification where available.

You can modify Correlation Details options on this page to customize the Bit9 information correlated with the notification. Your choices here affect all pages that display correlation options.

## Files On Computers Tab

This tab shows all instances of the files in this notification in the Bit9 Server file inventory. The can include (either by default or customization) all fields from the Bit9 Console Files On Computers page. You also can add External File Name and External Size columns. The Action menu has the same options as the Total Files tab menu.

You can modify Correlation Details options on this page to customize the Bit9 data correlated with the notification (this affects all pages that display correlation options).

## Directories Tab

For FireEye notifications, a Directories tab shows all relevant directory entries (i.e., paths where suspicious activity was identified) reported in the external notification. The table for this tab can include the following columns:

**Table 123:** Directories Tab Columns

Column	Description
Sequence	Sequence of each process's appearance when a suspected malware instance is analyzed in the network security device. The first process in the sequence is the top-level process.
Directory	Directory reported by the network security device (truncated to the right when displayed)
Operation	Operation on a directory (created, opened, deleted, etc.)
Process	Process reported by the network security device
Process MD5	MD5 hash of the process
Process Path	Path location of the process reported by the network security device

If a process that attempted access to the directory is known to the Bit9 Server, its listing here includes a View Details button, which opens the File Details page for this process.

The Action menu for this tab includes the following commands for selected files:

- **Ban Process Globally** – Bans process file(s) for all policies; requires no further configuration
- **Ban Process By Policy** – Opens a dialog box for creation of policy-specific and report-only bans
- **Remove Process Approval Or Ban** – Removes any active bans/approvals immediately.
- **Create Custom Rule** – Opens an Add Custom Rule page with pre-populated values to create a ban on the process attempting to access the directory. See [“Custom Rules for Directory Control”](#) for more details.

## Registry Keys

This tab shows all relevant registry value modifications reported in the External Notification. The table for this tab includes the following columns:

**Table 124:** Registry Keys Tab Columns

Column	Description
Sequence	Sequence of registry access attempts when a suspected malware instance is analyzed by the network security device.
Process	Process reported by the network security device.
Process MD5	MD5 hash of the process
Process Path	Path location of the process reported by the network security device
Key	Registry key reported by the network security device (truncated to the right when displayed)
Name	Registry field name reported by the network security device
Value	Registry field value reported by the network security device
Operation	Operation on a registry key (setval, added, etc.)

If a process that attempted access to the registry key is known to the Bit9 Server, its listing here includes a View Details button, which opens the File Details page for this process.

The Action menu for this tab includes the following commands for selected files:

- **Ban Process Globally** – Bans process file(s) for all policies; requires no further configuration
- **Ban Process By Policy** – Opens a dialog box for creation of policy-specific and report-only bans
- **Remove Process Approval Or Ban** – Removes any active bans/approvals immediately.
- **Create Registry Rule** – Opens an Add Registry Rule page with pre-populated values to create a rule to ban this process from accessing the registry keys reported in the notification. See [“Registry Rules”](#) for more details.

## More Details Tab

This tab shows additional details from the current external notification – the information included on this tab varies according to the type of the notification. The following table shows the possible fields:

**Table 125:** More Details Tab Fields

Field	Description
Malware type	Type of malware as reported in external notification; may be the same as Type in the External Notifications table or a more specific type, such as Backdoor, HackTool, Trojan, etc.
Anomaly	Anomaly
Application	Application targeted
HTTP Header	HTTP header(s) reported by an external notification for a web infection
Show XML Details	Opens a new browser tab with full XML notification from the external network security device. This alert is read from a file stored on the Bit9 Console web site (inside "store" subfolder). <b>Note:</b> Very large XML files may cause browser performance and navigation issues when you use this link to open them. One alternative is to right-click on the link and <b>Save Target/Link As</b> to a location where you can open the file with a different viewer.

## History Tab

The History tab provides an audit trail for external notification workflow. This includes each change of status and any comments associated with the change. In addition to clicking this tab when you are already on the Notification Details page, you display the history by clicking the History button in the Action column of the row for a notification on External Notifications table.

## Showing Related Notifications

If there are any notifications related to the one currently shown on the External Notification Details page, the Related Views menu includes a **Show Related Notifications** command. A related notification is one with the same MD5 hash as the currently shown notification.

When you click on this command, the External Notifications table opens, filtered to show the related notifications, including the one from which the link was clicked.

## Showing XML Details

External notifications are reported in XML format, and contain information about analyzed malware behavior. The Bit9 Server parses these XML notifications for efficient storage of key information in its database. In addition, the entire content of each XML notification is stored in a separate *store* folder for each network security device vendor in the Bit9 installation directory on the Bit9 Server (*Bit9\Integrations\PAN\store*, *Bit9\Integrations\CheckPoint\store* or *Bit9\Integrations\FireEye\listener\store*).

### Note

- Opening very large XML details files may cause browser performance and navigation issues. One alternative is to right-click the link and Save Target As or Save Link As to a location where you can open the file with a different viewer.
- If a notification from Palo Alto Networks includes reports for multiple “Analysis Environment” types, using Show XML shows only the XML details for the Analysis Environment of the current notification.
- XML Details links are not available for Microsoft SCEP notifications.

### To access the full XML details for an External Notification:

- On the External Notification Details page for the notification, click **Show XML Details** in the External Pages menu. The full details appear in a separate browser window.

## External Console Access

On the Notification Details page for most connectors, you can click on a command in the External Pages menu to open the console for the appliance that provided the notification. The console opens in a new browser window. If the user on the Bit9 Console is not already authenticated with credentials for the external appliance, the browser is redirected to a login page.

## Getting Malware Details

For Microsoft SCEP notifications, the External Pages menu on the Notification Details page is a link to the threat encyclopedia in the Microsoft Malware Protection Center, and displays the entry for the threat identified in the Malware Name field.

## Managing Notification Status

In the Bit9 Console, both the External Notifications table and the External Notification Details page show a *status* field for each notification. Notification Status is strictly a means for tracking the progress of your response to a notification and does not communicate status changes back to the notification source. There is no mandatory flow of notification status, but the following might be a useful template for status workflow.

**To manage the status of a notification:**

1. On the console menu, choose **Reports > External Notifications** and click the View Details button next to the notification you want to review. The External Notification Details page opens.
2. On the External Notification Details page, if you intend to examine and/or take action on this notification, choose **Escalate Notification** in the Actions menu. The status changes to Escalated.
3. Research the notification using the information on the External Notification Details page, the File Details page, the Event pages, the network security device analysis of a file, or any other means appropriate for the notification. Provide any comments related to the escalation in the Comments field.
4. Take whatever action you choose to take on the files in the notification, for example, banning files or creating custom or registry rules.  
**Note:** Bans or other rule changes do not affect the Status field of the request itself. You must change status manually.
5. Provide any comments related to the resolution in the Comments field.
6. Once you have taken action, or if you determine that no action is necessary, choose **Resolve Notification** in the External Notification Details Action menu. The status changes to Resolved.
7. When you are finished with this notification, make any final comments in the Comments field and then choose **Close Notification** in the Actions menu. The status changes to Closed and the view returns to the External Notifications table. Closing a notification removes it from the **Active Notifications** view, but it is visible if you choose a Saved View of **(none)**.

The steps above describe Status being changed from the Actions menu on the External Notification Details page. You also can change status using the Status dropdown menu on that same page, and from the Action menu on the External Notification page table.

## Banning Externally Reported Malware

The Bit9 Server can ban files or processes reported as part of a malware notification by external network security devices. There are several ways in which this can be done:

- **Manual file bans** of files reported in external notifications
- **Registry Rules** that ban certain processes that attempt access to registry keys, as reported in external notifications
- **Custom Rules** that ban activity in a directory reported in external notifications
- **Event Rules** that automatically create report-only bans or other rules when certain file-related events occur, in this case, due to external notifications

Registry, Custom, and Event rules can also be configured to *report* the actions they describe rather than banning them.

### Manually Banning Files

You manually ban files reported in external notifications much the same way you would any Bit9-inventoried file. However, you can apply bans directly from the External Notification Details page Action menu, so you can ban malware identified in an external notification, whether or not it has appeared yet on a Bit9-Agent-managed endpoint.

**To manually ban files reported as malware in an external notification:**

1. Click the View Details button next to the notification whose files you want to ban.
2. On any of the Files tabs on the External Notification Details page, check the box to the left of each file you want to ban.
3. On the Action menu, choose the ban type you want to apply to the checked files:
  - a. Choose **Ban Globally** to ban the file for all computers. This creates the ban without requiring any further interaction.
  - b. Choose **Ban by Policy** to customize the ban. This opens the Add File Rule page with information partially filled in. On this page, you can choose a fully functional ban or a Report Only ban, and you can choose specific policies to which the ban will apply. Report Only bans are useful if you want to monitor what an active ban *would* do before fully enabling it. When you have configured the ban, click **Save**.

**Note:** The Action menu on the Files tabs on the External Notification Details page include the following choices for finding a file of interest:

- **Find by Name**
- **Find by Size**
- **Find by Hash**

The Files tab of the Software Rules page (**Rules > Software Rules** on the console menu) shows bans you have created. Bans manually created from an external notification are named with a prefix of “External\_” followed by the file name.

**Note:** Some External Notification pages allow you to ban the *process* that attempted to perform an action on an object on your systems, such as modifying a registry key or writing to a directory. You can ban those processes using the same procedure described above, except that the commands will say *Ban Process* instead of just Ban.



## Special Rules for Reporting or Banning Malware

For certain notifications, standard file bans may not provide the best remediation. The Bit9 Connector offers several other rules to control actions that are identified as suspicious. As with bans, these rules can be created from the External Notification Details page with some of the rule data pre-populated.

### Registry Rules

If a notification includes suspicious registry entries or activity, its External Notification Details page includes a Registry Keys tab. This tab provides information about the keys that might be compromised. You can select one or more of the reported keys and:

- Ban the process that tried to access the key
- Remove previously created process bans or approvals
- Create a Registry Rule to control access to the key

Bans created in this context are similar to those created on any of the Files tabs. The Registry Rule command provides different options.

#### To create a Registry Rule from a Notification Details page:

1. In the Notification Details page of interest, click on the **Registry Keys** tab.
2. Check the boxes next to the registry keys for which you want to create a rule.
3. On the Action menu, choose **Create Registry Rule**. The Add Registry Rule page appears, with rule name and settings pre-populated with details from the notification.
4. By default, a rule created in this way blocks writes to the named registry keys by the processes identified in the notification, and does this for all users and all policies. You can modify these settings before you save the rule. Among the options on the Write Action menu, you can choose **Report**, which means that activity at this key is reported but not blocked. If you are unsure of how best to configure a rule, see [“Creating Registry Rules”](#) on page 391. You can **Cancel** the rule without saving it if you would like to investigate rules parameters first.
 

**Important:** Rule menus have options that *Allow* activity at the named locations and even *Promote* processes to have more privileges than they previously did. If you alter the pre-populated values, be careful of the choices you make on these menus.
5. Modify the rule as you choose, and then click the **Save** button. The new rule is created and appears on the Registry tab of the Software Rules page in the Bit9 Console.

### Custom Rules for Directory Control

Notifications that include suspicious pathname entries have a Directories tab on their External Notification Details page, providing information about the directories that might be compromised. On this tab, you can select one or more keys and:

- Ban the process that tried to access the directory
- Remove previously created process bans or approvals
- Create a Custom Rule to control access to this location

Process bans created in this context are similar to file bans created on any of the Files tabs. The Custom Rule command provides different options.

**To create a Custom Rule from a Notification Details page:**

1. In the Notification Details page of interest, click on the **Directories** tab.
2. Check the boxes next to the Directories for which you want to create a rule.
3. On the Action menu, choose **Create Custom Rule**. The Add Custom Rule page appears, with its name and settings already filled in with details from the External Notification.
4. By default, a rule created in this way blocks writes to the named directories by the processes identified in the notification, and does this for all users and all policies. You can modify these settings before you save the rule. Among the options on the Execute Action menu, you can choose **Report**, which means that activity at this location is reported but not blocked. If you are unsure of how best to configure a rule, see [“Creating a Custom Rule”](#) on page 338. You can **Cancel** the rule without saving it if you would like to investigate rules parameters first.  
**Important:** Some options on the rule menus that *Allow* activity at the named locations and even *Promote* processes to have more privileges than they previously did. If you alter the pre-populated values, be careful of your choices on these menus.
5. Modify the rule as you choose, and then click the **Save** button. The new rule is created and appears on the Custom tab of the Software Rules page in the Bit9 Console.

## Analysis of Suspicious Files on Endpoints

If you have enabled integration and file analysis with an external device or service, you can submit files from the Bit9 Server file inventory to the connected source for analysis. With analysis enabled, the Bit9 Console adds **Analyze with...** commands to menus in several locations that allow you to submit files to appliances or services from Palo Alto Networks, Check Point, or to FireEye. For Check Point and FireEye, these commands have Windows-version-specific submenus so that you can choose the environment in which you want the file analyzed. The locations for these commands are:

- File Catalog, Files on Computers and Find Files Results pages Action menus (for one or more files)
- File Details and File Instance Details Advanced menus (for one file)
- Events page Action menu (for one or more files)
- Other table pages that list files

### Note

A file in the Bit9 file inventory might be unavailable, either temporarily, because it is inaccessible on the network, or permanently, because it was deleted or was a transient file. If you attempt to send such a file to an external device for analysis, when it is not found, Bit9 will attempt to locate another instance of the same file and send that file for analysis. If no other instance exists, the analysis request will produce an error.

**Platform Note:** File analysis via the Bit9 Connector currently is supported for files from Windows agents.

**To submit files to an external service for analysis:**

1. In a table that lists files, check the boxes next to files you want to submit.
2. On the Action menu choose from the available **Analyze with** commands – the available commands depend upon the appliances you have enabled for the connector:
  - a. If you have enabled the Palo Alto Networks-Bit9 for file analysis, you can choose **Analyze with Palo Alto Networks WildFire**.
  - b. If you have enabled the Check Point-Bit9 integration for file analysis, you can choose the **Analyze with Check Point** submenu and under it, the analysis environment in which you want the file analyzed, which includes the operating system and other common tools such as Microsoft Office and Adobe Acrobat (for example **win7;Office 2010;Adobe 9**).
  - c. If you have enabled FireEye-Bit9 integration for file analysis, you can choose the **Analyze with FireEye** submenu and under it, the operating system in which you want the file analyzed (for example **win7**). The exact names and choices of operating system will depend on how your FireEye environment was set up.

A message will appear indicating that the files have been scheduled for upload to the analysis source you chose.

3. Alternatively, you can go to a File Details or File Instance Details page for a single file and choose an **Analyze with** command on the Advanced menu.

From these pages, if a file has already been submitted to the same analysis provider, a warning is shown, but the file will be uploaded again if you click **OK** on the warning.

4. To monitor the progress of the analysis, choose **Tools > Requested Files** and click on the **Analyzed Files** tab to see the table of files submitted.

## Monitoring Files Submitted for Analysis

In the Bit9 Console, the Analyzed Files tab of the Requested Files page shows the status and (if complete) analysis results for all files submitted to external services for analysis. The default view for this page shows all files sorted by request date, but there also are Saved Views available that can provide a more targeted list of files:

- Analysis in Progress
- Completed Analysis
- Analysis Errors
- Files Submitted to Check Point
- Files Submitted to FireEye
- Files Submitted to WildFire

Action	Request Date	Status	Target	Analysis Result	Computer	File Name
<input type="checkbox"/>	May 17 2013 03:28:20AM	Acquiring File	Palo Alto Networks WildFire		MYCORP\Desktop-4	gdump.exe
<input type="checkbox"/>	May 17 2013 03:28:20AM	Analyzed	Palo Alto Networks WildFire	Malicious	MYCORP\Desktop-1	icar.com
<input type="checkbox"/>	May 17 2013 03:27:17AM	Canceled	FireEye:win7		MYCORP\Laptop-3	unbootloader.exe

The table can show the following columns (not all are shown by default):

- **Request Date** – When the request for file analysis was submitted for this file.
- **Requester** – The user who requested the upload.
- **Upload %** – The percent complete of the upload (not the analysis).
- **Status** – This indicates where in the analysis process this file is. See “[Analysis Status](#)” for a description of status values.
- **Analysis Results** – When the analysis is completed, this field indicates the result of the analysis (Clean, Potential Risk or Malicious).
- **Computer** – The computer from which the file was uploaded.
- **File Name** – The name of the file in the location from which it was uploaded.
- **File Size** – The size of the file as it appears (or appeared) on Bit9-Agent-managed computers.
- **MD5** – The MD5 hash of the file.
- **Date Modified** – The last time the entry for this file was changed.
- **Error** – Any error associated with the upload or submission for analysis of the file.
- **File Path** – The directory where the file resided on the source computer at the time the file was uploaded - it is not necessarily the current location of the file.
- **Last Modified By** – Who last modified the Analyzed Files entry for this file by taking a related action.
- **Prevalence** – The prevalence of this file on Bit9-managed computers.
- **Provider** – Palo Alto Networks or FireEye
- **SHA-256** – The SHA-256 hash of this file.
- **Source** – The source of this analysis request. Can be "Manual" or "Event rule".
- **Source Name** – If the source was "Event rule", the name of the rule.
- **Target** – The target for the file analysis. This will be **Palo Alto Networks WildFire**, **Check Point**:<Target Environment> or the **FireEye**:<Windows version> choice specified by the user who initiated the analysis. For Check Point and FireEye analysis done on a local appliance, this field also shows the appliance name. For example:  
**Check Point**:win7;Office2010;Adobe9:Appliance1

Files from the Bit9 Agent that are targeted for analysis are not stored on the Bit9 Server and cannot be downloaded to the server or deleted from this table.

## Analysis Status

On the Analyzed Files tab, the Status column provides feedback on the progress of a file analysis. Hovering over the Status value in the table provides additional information. The possible values are:

- **Acquiring File** – For files that must be uploaded from an endpoint before being sent to the device for analysis, this indicates that the upload has not been completed.
- **Error** – The upload or analysis failed (e.g., because the file name or path did not exist). Moving the mouse cursor over this field shows a tooltip with details of the error.
- **Canceled** – The upload was canceled by a console user.
- **Analyzing** – The file has been moved to a device for analysis.
- **Analyzed** – The Bit9 Server has received an XML report from the device. Once this happens, the Status value for the file becomes a link leading to Notification Details.
- **Analyzed\* (1,2...)** – When Analyzed is followed by a series of numbers in parentheses, this indicates that there were multiple file analysis results from WildFire. Each result is from a different “Analysis Environment”. Hovering the mouse cursor over a number shows the Analysis Environment it represents.

Status	Target	Analysis Result
Analyzed*(1,2)	Palo Alto Networks WildFire	Clean
Analyzed*(1)	Palo Alto Networks WildFire	Malicious
Analyzed	Palo Alto Networks WildFire	Malicious

Clicking on a number shows the specific Notification Details for that Analysis Environment. See [“Notifications from Multiple Analysis Environments”](#) on page 724 for more on the possible values.

The Analysis Results for a file that has multiple results reports the top-level analysis value provided by WildFire.

### Note

If there are analysis results for a file, they appear in an External Analysis Results panel on the File Details and File Instance Details pages for that file.

## Actions on the Analyzed Files tab

The Action menu on the Analyze tab provides options for you to retry an analysis request with the same or different analysis provider. It includes the following options:

- **Cancel Analysis** – Cancels checked analysis entries. If one or more checked entries cannot be canceled, this will have no effect on those files.
- **Retry Analysis** – Retries checked analysis entries. This has no effect on entries that cannot be retried (for example, because analysis is already pending on this file).
- **View Bit9 SRS Cloud Data** – Get information (if available) from Bit9 SRS for the checked files.

- **Analyze with ...** – Options appear for each available analysis provider (Check Point, Palo Alto Networks WildFire, and FireEye). For Check Point and FireEye, there are options to target the submission to the appropriate operating system.

When one of these actions is chosen, the submission for analysis will use an existing uploaded file if available. If not, it will first upload file, and then submit it.

#### Note

In addition to the Analyzed Files tab, the Requested Files page has two other tabs not described in this appendix:

- **Uploaded Files** – Shows inventoried files uploaded from Bit9-managed endpoints to the Bit9 Server.
- **Diagnostic Files** – Shows diagnostic files uploaded to the Bit9 Server.

See [Appendix E, “Uploading Files from Agents,”](#) for a full description of general and diagnostic file uploads.

## Bit9 Logging of Connector-related Events

The Bit9 Events page provides access to all recorded events related to Bit9 activities in your environment, including files blocked, unapproved files executed, system management processes and actions by console users. The Bit9 Server updates its event data in near-real-time for connected computers, with minor variations due to event volume. See [“Event Reports”](#) on page 482 for more details.

You can optionally choose to direct the Bit9 Syslog event output for post-processing on another system. See [“Event Management Options”](#) on page 617 for more details.

When the Bit9 Connector for Network Security Devices is enabled, connector-related events appear in the Bit9 event log. There are several key additions or changes to Bit9 events due to the integration with network security devices:

- **External Notification** – This event subtype (*subtype* is the most specific identifier for an event) is under the Discovery type. It is generated for external notifications (currently from Check Point, Palo Alto Networks, or FireEye) received by the Bit9 Server. However, it is not generated for an external notification that is received as a result of a file submission if a File Analysis Complete is also generated.
- **Connector Actions in Other Events** – Other events that can report connector-related activity are shown in [Table 126](#). Most of these event subtypes are also used for other purposes – descriptions that could appear for the subtype but are not related to network security device activity are not shown here. See the separate *Bit9 Events Guide* for a complete description of all event types and subtypes in Bit9 and how to enable Syslog event output.

**Table 126:** Connector-Related Events in the Bit9 Event Log

Event Type	Event Subtype	External Notification-Related Description and Samples
Discovery	Malicious file detected	Unknown file '\$filename\$' [\$param1\$] was identified by \$param3\$ as malicious. or File '\$filename\$' [\$param1\$] was identified by \$param3\$ as malicious.
Discovery	Potential risk file detected	Unknown file '\$filename\$' [\$param1\$] from \$param3\$ was identified by \$param3\$ as potential risk. or File '\$filename\$' [\$param1\$] from \$param3\$ was identified by \$param3\$ as potential risk.
Discovery	External Notification	\$Provider\$ reported \$malware type\$ with name \$malware name\$ for file '\$filename\$' from \$src_ip\$ to \$target_ip\$
Computer Management	File Upload Requested	User '\$username\$' requested upload of file [\$hash\$] from computer '\$computer\$'. or User '\$username\$' requested upload of file '\$param1\$' from computer '\$computer\$'. or Upload of file [\$hash\$] from computer '\$computer\$' was requested by event rule '\$ruleName\$'.  <b>Note:</b> Reported uploads could be unrelated to External Notifications.
Computer Management	File Upload Completed	Upload of file [\$hash\$] from computer '\$computer\$' completed. or Upload of file '\$param1\$' from computer '\$computer\$' completed.
Computer Management	File Upload Canceled	User '\$username\$' canceled upload of file [\$hash\$] from computer '\$computer\$'. or User '\$username\$' canceled upload of file '\$param1\$' from computer '\$computer\$'.
Computer Management	File Upload Error	Upload of file [\$hash\$] from computer '\$computer\$' failed because of error '\$param2\$'. or Upload of file '\$param1\$' from computer '\$computer\$' failed because of error '\$param2\$'.

Event Type	Event Subtype	External Notification-Related Description and Samples
Computer Management	File Upload Deleted	User '\$username\$' deleted uploaded file [\$hash\$]. or User '\$username\$' deleted uploaded file '\$param1\$'.
General Management	Event rule created	Event rule '\$param1\$' has been created by '\$userName\$'.
General Management	Event rule modified	Event rule '\$param1\$' has been modified by '\$userName\$'.
General Management	Event rule deleted	Event rule '\$param1\$' has been deleted by '\$userName\$'.
Server Management	File analysis requested	User '\$username\$' requested analysis of file [\$hash\$] with '\$param1\$'. or Analysis of file [\$hash\$] with '\$param1\$' was requested by event rule '\$ruleName\$'.
Server Management	File analysis completed	File '\$filename\$' [\$hash\$] was successfully analyzed with '\$param1\$'. Nothing suspicious was found. or File '\$filename\$' [\$hash\$] was successfully analyzed with '\$param1\$'. It was reported as malicious.
Server Management	File analysis canceled	User '\$username\$' canceled analysis of file '\$filename\$' [\$hash\$] with '\$param1\$'.
Server Management	File analysis error	Analysis of file '\$filename\$' [\$hash\$] with '\$param1\$' failed because of error '\$param2\$'.
Server Management	Server error	\$param1\$ <b>Note:</b> This is not specific to connectors but may report connector-related errors, such as failure to connect to or authenticate with a device.
Server Management	Connector restart	Connector started, build information: \$param1\$.
Server Management	Connector shutdown	Connector shutdown cleanly.

## Additional Log Information

In addition to the Bit9 event log, you may be interested in information available in the log files for the connector integrations. This information is located in the following locations under the Bit9 installation folders:

- **For Check Point** – `\Bit9\Integrations\CheckPoint\B9ConnectorCP.bt9`
- **For FireEye** – `\Bit9\Integrations\FireEye\listener\debug.log`.
- **For Palo Alto Networks** – `\Bit9\Parity Server\Reporter\ParityReporter.log`



## Appendix D

**Diagnostic Files****Sections**

Topic	Page
<a href="#">Overview</a>	742
<a href="#">Uploading Agent Diagnostic Files</a>	742
<a href="#">Viewing Diagnostic Files</a>	743

## Overview

The Bit9 Console includes a page that displays certain diagnostic files for the Bit9 Server and Bit9 Agents. These files can be useful when you are investigating issues in your Bit9 environment with the assistance of Bit9 Support.

Diagnostic files appear on the Diagnostic Files tab of the Requested Files page, and include:

- Server Installation Logs and dump files
- Agent diagnostic files requested by console users

Server installation log and dump files appear automatically on the tab when server activity causes them to be created. Agent diagnostic files must be requested through the Computers or Computer Details page. Once uploaded to the server, these files may be downloaded to any computer running the Bit9 Console.

Unlike the ability to select and upload any file from an agent, access to diagnostic files is available without a special license or permissions.

### Note

This appendix describes *diagnostic file* uploads only. For information about uploading other files from an agent, see [Appendix E, “Uploading Files from Agents.”](#) This capability requires a separate license.

## Uploading Agent Diagnostic Files

Agent diagnostic files uploads can be initiated from the Computers page or the Computer Details page. On the Computers page, you can upload files from one or more computers.

### To initiate a diagnostic file upload from one agent:

1. On the console menu, choose **Assets > Computers**. The Computers page appears.
2. Find the computer whose statistics or diagnostic information you want to upload and open its details page.
3. On the Computer Details page, choose **Other Actions** in the Advanced menu, and on the Other Actions menu, choose **Upload diagnostic files**.

Unless a problem is encountered, a message on the Computer Details page indicates that the upload of the file you chose has been scheduled. You can check the Diagnostic Files tab to see whether a new zip file for this agent is available yet.

### To initiate diagnostic file uploads for one or more agents:

1. On the console menu, choose **Assets > Computers**. The Computers page appears.
2. Check the box next to each computer for which you want to upload diagnostics, then choose **Upload diagnostic files** on the Action menu. A confirmation dialog appears.
3. Choose **OK** on the confirmation dialog to begin the upload. A status message indicates whether the request was successful and indicates how many computers will be sending diagnostic files to the server.

## Canceling or Retrying an Upload

If an upload has not been completed, you can cancel it. This might be a choice you want to make if you inadvertently chose more computers than you actually wanted when you initiated the upload, or if the file size shown in the table is excessively large.

### To cancel diagnostic file uploads:

1. On the console menu, choose **Tools > Requested Files**.
2. Click on the **Diagnostic Files** tab. The table shows diagnostic files that have been uploaded, are in the process of uploading, or were requested but not uploaded.
3. Check the box next to each file whose upload you want to cancel and choose **Cancel Uploads** from the Action menu.
4. Choose **OK** on the confirmation dialog.

If an upload has failed or been canceled, you can Retry it by checking its box on the Diagnostic Files page and choosing **Retry Uploads** on the Action menu.

## Viewing Diagnostic Files

Diagnostic files are listed in the table that appears on the Diagnostic Files tab of the Requested Files page.

### To view diagnostic files:

1. On the console menu, choose **Tools > Requested Files**.
2. Click on the **Diagnostic Files** tab. Any diagnostic files uploaded to the server are shown in the table.

The screenshot shows a web interface titled "Requested Files: Diagnostic Files". It has three tabs: "Uploaded Files", "Analyzed Files", and "Diagnostic Files". Below the tabs are controls for "Saved Views" (set to "(none)"), "Group By" (set to "(none)" with "Ascending" selected), and a toolbar with "Show/Hide Filter", "Show/Hide Columns", "Export to CSV", and "Refresh Page". An "Action" dropdown menu is visible above a table. The table has columns: File Type, Request Date, Priority, Requester, Status, Computer, File Name, and File Size. Two rows are shown:

File Type	Request Date	Priority	Requester	Status	Computer	File Name	File Size
<input type="checkbox"/> Agent Diagnostics	Apr 14 2015 07:32:20 AM	Medium	admin	Uploaded	MYCORP\LT3	R3-diagnostics-20150414-0732170054.zip	49 MB
<input type="checkbox"/> Server Diagnostics	Apr 10 2015 10:19:00 AM	Medium		Uploaded	System	ServerInstall-2015410-094526.log	266 KB

At the bottom of the interface, it shows "2 items", "Page 1/1", and a "25 rows per page" selector.

When you request a diagnostic file upload from an agent, a zip file is uploaded to the server with diagnostic and log files relevant to the agent. For example, on Windows systems, the zip file includes the Bit9 Agent Logs folder (ProgramData\Bit9\Parity Agent\Logs) and selected log files from the Windows folder. The exact files included in the zip file vary by operating system platform.


Uploaded diagnostic files are named in the following format:

*<computername>-diagnostics-<date>-<time>.zip*

Server diagnostics files may be **.log**, **.dmp**, or other formats.

Table 127 shows the columns available for the Diagnostic Files page, some of which appear by default and some of which you must add.

**Table 127:** Diagnostic Files Table Columns

Column	Description
Actions	<p>The Action column includes a checkbox for choosing files on which Action menu commands will act and buttons for taking action on individual files. The Action menu on this page includes the following commands:</p> <ul style="list-style-type: none"> <li>• <b>Cancel Uploads</b> – Cancel the upload of checked files (if the upload has not been completed).</li> <li>• <b>Retry Uploads</b> – Retry the upload of checked files.</li> <li>• <b>Delete Uploads</b> – Delete the table rows for checked files, and, for successful uploads, delete the files from the server.</li> </ul> <p> Download the file (if it was successfully uploaded) from the Bit9 Server to the computer on which the console is being viewed.</p>
Priority	Priority in which pending files are uploaded to the server. For diagnostic files, the priority is always <b>Medium</b> .
Request Date	When the file upload was requested.
Requester	The console user that requested the upload, or blank if the file is a server log.
Status	<p>The status of the file upload. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Uploaded</b> – The upload completed successfully and the file is available on the server.</li> <li>• <b>Uploading</b> – The upload is in progress but not yet complete; a partial file has been received by the server. This status is likely to appear only for very large files.</li> <li>• <b>Initiated</b> – The upload task has been received by the agent where the file is located.</li> <li>• <b>Queued</b> – The upload task has not yet been sent to the agent.</li> <li>• <b>Error</b> – The upload failed. Hovering the cursor over this status displays the error message. Errors include: No file with hash, The system cannot find the path specified, The system cannot find the file specified.</li> <li>• <b>Canceled</b> – The upload was cancelled by a console user.</li> </ul>
Computer	The name of the computer from which the file was uploaded.
File Name	The name of the uploaded file.
File Size	The size (in bytes) of the file.
Upload %	The percent of the upload that is finished. Completed uploads show 100%. Failed uploads and uploads not yet started show 0%.
Upload Date	When the file was uploaded to the server.

Column	Description
Upload Directory	The directory on the Bit9 Server to which the file was uploaded. Value is "(default)" for manual uploads, which use the directory configured in the System Configuration Advanced Options tab. If the upload is due to an event rule, the actual path is shown.
Error	A description of the error that prevented the file from uploading. Not shown by default.
File Path	The location on the agent computer from which the file was uploaded. Not shown by default.
Prevalence	The number of Bit9-managed computers reporting to your server on which this file is present.
MD5	The MD5 hash of the file.
SHA256	The SHA-256 hash of the file.
Source	Source of the request for upload. Either "Event rule" or "Manual".
Source Name	If the request was due to an event rule, the name of the rule. If the request was manual, this field is empty.

## Deleting Uploaded Diagnostic Files

When you no longer need a diagnostic file, you can delete it from the server by checking the box next to its row on the Diagnostic Files page and choosing Delete Uploads from the Action menu.



## Appendix E

# Uploading Files from Agents

**Sections**

Topic	Page
<a href="#">Overview</a>	748
<a href="#">Enabling Access to File Upload Features</a>	748
<a href="#">Scheduling Uploads</a>	749
<a href="#">Viewing the Uploads Table</a>	752
<a href="#">Downloading Uploaded Files</a>	755
<a href="#">Deleting Uploaded Files</a>	755

## Overview

In all active modes, the Bit9 Security Platform provides the ability to monitor the propagation of software and generate audit trails of activity. In some cases, information you see during monitoring might lead to a need to access the actual file involved in certain activities. The optional Upload Files feature provides the ability to upload a copy of any file to the Bit9 Server from a computer running Bit9 Agent 7.0.0 or later.

Access to the Upload Files feature requires application of a special license key, either for File Uploads alone or as part of the Bit9 Connector license. See [“Managing Bit9 Platform Licenses”](#) on page 640 for instructions on applying Bit9 licenses.

### Notes

The ability to send a file to third-party devices or services for analysis uses the File Upload feature. However, uploads due to a request for analysis are not displayed in the file upload user interface, and are not discussed here. See [Appendix C, “Bit9 Connector for Network Security Devices,”](#) for information on the process involved in uploading files for analysis.

Diagnostic files may be uploaded from agent computers, and in special cases, from the server. These are cataloged on a separate tab from general file uploads, but much of the user interface for acting on them is the same.

## Enabling Access to File Upload Features

### Important

- Permission for these features is *not* granted by default to the *admin* account or members of the *Administrator* account group. You must explicitly add these permissions.
- While other Bit9 features provide data *about* files on agent-managed computers, these features allow a console user with the appropriate privileges to upload the actual file. These features should be used with extreme care, and in full compliance with your organization's policy on accessing other user's files. Be sure that only those Bit9 Console users that absolutely need access to the features are given permission to use them.

The following permissions control access to File Upload features:

- **Tools/View file uploads** – Ability to view uploaded files on the Requested Files page.
- **Tools/Manage uploads of inventoried files** – Ability to initiate manual file uploads from agent computers, and to create event rules that upload files. This permission applies only to files considered “interesting” (i.e., executables and scripts) by Bit9.
- **Tools/Manage uploads of files by pathname** – Ability to initiate manual file uploads from agent computers. This permission enables uploading of a file by its pathname, even if not in the Bit9 inventory.
- **Tools/Access uploaded files** – Ability to download files uploaded to the server.

See [“Account Group Permissions”](#) on page 93 for details on enabling feature access.



## Scheduling Uploads

Several locations in the Bit9 Console provide access to commands for manually uploading files, including:

- the Events page (for events showing files that exist on computers)
- the Approval Requests page
- the File Catalog and Files on Computers tables
- the Find File Results table
- the Snapshot Contents table
- the File Details and File Instance Details pages
- the Computer Details page (for uploading a file by path only)

From most of these pages, you can upload a copy of any file that has been identified as "interesting" (i.e., executable) by Bit9 and has been added to the live inventory. From the Computer Details page, you can upload a copy of *any* file on the computer, whether or not it exists in your Bit9 file inventory. For all uploads, the original file remains on the agent computer. Note that there are separate permissions for uploading files from the inventory and uploading any file by path.

### Important

Uploading files greater than 2 gigabytes is not recommended. Files in excess of 2GB may fail to upload and show a "communication error".

In addition to performing manual uploads, you can create Event Rules that upload files when certain events take place. See [“Event Rules”](#) on page 423 for more information.

When you issue a successful upload command, a message appears on the console page indicating that the upload has been scheduled. In general, uploads begin almost immediately, but there could be delays depending upon other activities on the Bit9 Server and the size of the file you are uploading. Also, the Bit9 Server needs at least read permission to upload the file, and some files that are opened by other programs cannot be uploaded. If the Bit9 Server does not have read permission for a requested file on any agent-managed computer, the Uploaded Files table shows an error message for that file.

If an upload is scheduled for a file and no computer with that file is currently connected, the upload will be attempted later. Also, if a file upload is interrupted because of an agent-side error, it will be retried.

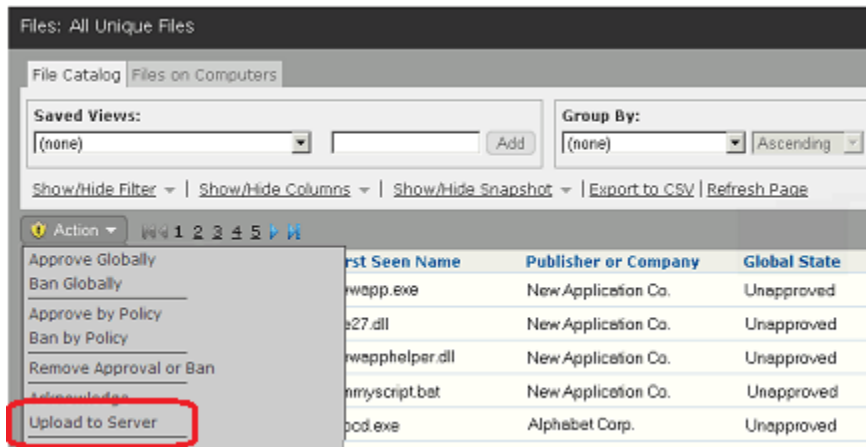
## Starting Uploads of Inventoried Files from Tables

You can schedule the upload of one or more files at a time from the tables pages that include file links (File Catalog, Files on Computers, Events, etc.). When you request an upload, the Bit9 Server chooses the computer from which to upload a file matching the hash. It first searches for an instance of the file on a currently connected computer. If there are multiple connected computers with the file, the “best” computer is chosen based on how recently it communicated with the server and whether any other uploads are scheduled or in progress (avoiding these is preferable). If the file does not exist on a

connected computer, the server schedules the upload from a disconnected computer, and will start the upload when that computer reconnects.

**To initiate a file upload from a file table:**

1. Navigate to the file table page, such as Files on Computers.
2. Check the box(es) next to the file(s) you want to upload to the server.
3. On the Action menu, choose **Upload to Server**.



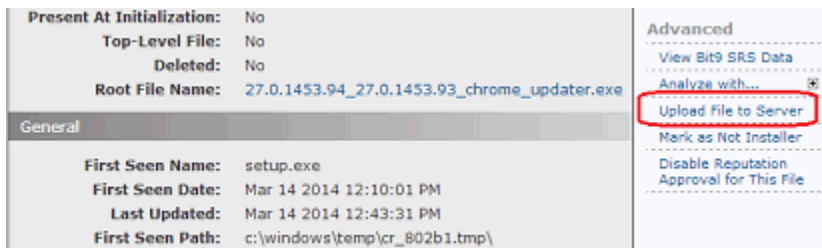
4. On the confirmation dialog, click **Yes**.  
A message appears on the page indicating that the upload has been scheduled.

**Starting Uploads from the File Instance Details Page**

You can schedule the upload of a single file from the File Instance Details page or the File Details page. The procedure is the same.

**To initiate a file upload from the File Instance Details page:**

1. Navigate to the File Instance Details page for the file you want to upload.
2. On the Advanced menu to the right of the file data, choose Upload File to Server.



A message appears on the page indicating that the upload has been scheduled.

Once you upload a file from a Details page, the Upload File to Server command on the Advanced menu changes to **Related File Uploads**. Clicking on this link opens the Requested Files page to the Uploaded Files tab, and filters it for the SHA-256 hash of this file.

## Starting Uploads by Path from the Computer Details Page

You can schedule the upload of any file on a computer from its Computer Details page, whether or not the file exists in your Bit9 file inventory of "interesting" files. Unlike uploads from other console pages, you must provide the path to the file – there is no list of files to choose from, and the upload is not based on a hash.

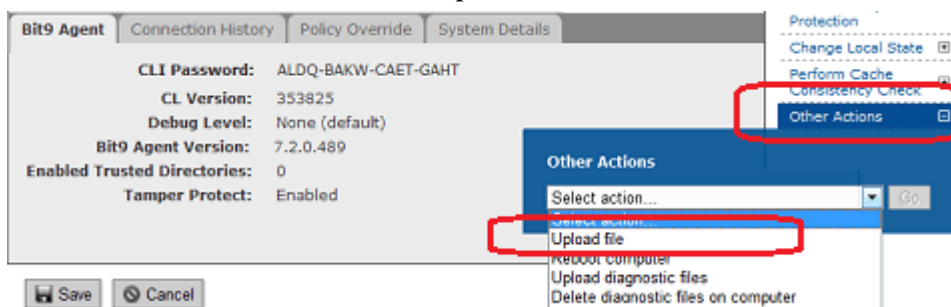
### Note

The ability to upload files via the Computer Details page requires a separate account permission – *Manage uploads of files by pathname*. See [“Account Group and Access Privileges”](#) on page 76 for instructions on setting this permission.

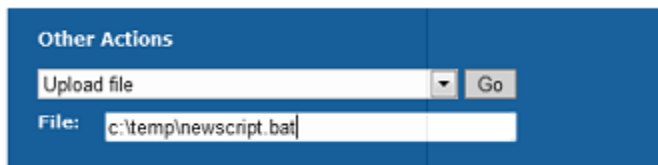
Although wildcards may not be used in the path to a file, you can specify the path location using macros and registry keys. See [“Using Macros”](#) on page 347 for the list of path macros recognized by Bit9.

### To initiate a file upload from the Computer Details page:

1. Navigate to the Details page for the computer that has the file you want to upload.
2. On the Advanced menu to the right of the file data, choose **Other Actions**.
3. On the Other Actions menu, choose **Upload File**



4. In the File box that appears in the menu, enter the complete path to the file you want to upload and then click the **Go** button.



A message appears on the page indicating that the upload has been scheduled. If you enter a non-existent file or path, the upload is still attempted, and you will not see an error on the page from which you initiate the upload, but a record of the failed attempt will appear in the Requested Files/Uploaded Files table.

## Viewing the Uploads Table

Each requested upload appears on the Uploaded Files page, even when it fails. From this page, you can view information about the uploaded file, delete the upload from the list, retry the upload, cancel uploads in progress, and view the uploaded file.

### To open the Uploaded Files page:

1. On the console menu, choose **Tools > Requested Files**.
2. If the Requested Files:Uploaded Files view is not already showing, click on the **Uploaded Files** tab.

The screenshot shows the 'Requested Files:Uploaded Files' interface. At the top, there are tabs for 'Uploaded Files', 'Analyzed Files', and 'Diagnostic Files'. Below the tabs, there are sections for 'Saved Views' (currently set to '(none)') and 'Group By' (set to '(none)' with an 'Ascending' sort order). There are also links for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', and 'Refresh Page'. An 'Action' dropdown menu is visible above the table. The table itself has the following data:

	Request Date	Requester	Status	Computer	File Name	File Size
	Jun 17 2013 03:33:30PM	bjones	Uploaded	MYCORP\LAPTOP-1	wp.exe	20 KB
	Jun 17 2013 01:50:32PM	System	Error	MYCORP\LAPTOP-6	setup.exe	1 MB


At the bottom of the table, it indicates '2 items', 'Page 1/1', and a '25 rows per page' setting.

On the Uploaded Files page, in addition to the default view, you can choose from among the following Saved Views:

- Uploads in Progress
- Completed Uploads
- Upload Errors

[Table 128](#) shows the columns available for the Uploaded Files page, some of which appear by default and some of which you must add.

**Table 128:** Uploaded Files Table Columns

Column	Description
Actions	<p>The Action column includes a checkbox for choosing files on which Action menu commands will act and buttons for taking action on individual files. The Action menu on this page includes the following commands:</p> <ul style="list-style-type: none"> <li>• <b>Cancel Uploads</b> – Cancel the upload of checked files (if the upload has not been completed).</li> <li>• <b>Retry Uploads</b> – Retry the upload of checked files.</li> <li>• <b>Delete Uploads</b> – Delete the table rows for checked files, and, for successful uploads, delete the files from the server.</li> <li>• <b>Change priority to:</b> – Change the priority of this upload request to one of the choices on the menu. The choices are <b>Low</b>, <b>Medium</b>, <b>High</b>, and <b>Highest</b>. Changing priority affects the order in which any pending files are uploaded.</li> <li>• <b>View Bit9 SRS Cloud Data</b> – View any data available in the Bit9 SRS database for this file (identified by hash)</li> <li>• <b>Analyze with ...</b> – If any third-party analysis devices or services are integrated through the Bit9 Connector, you can send selected files to them for analysis. For files that were not successfully uploaded to the Uploaded Files page, choosing an Analyze command initiates a new upload, and if that is successful, the file is submitted to the third-party device.</li> </ul> <p>Individual uploaded file rows may be acted upon by the buttons in their row. These include the standard File Details and Find File buttons found in all file tables. There is one additional button for successfully uploaded files:</p> <p> Download the file (if it was successfully uploaded) from the Bit9 Server to a specified location. For this, console users must have specific permission to access uploaded files.</p>
Priority	Priority in which pending files are uploaded to the server. The priority choices are <b>Low</b> , <b>Medium</b> , <b>High</b> , and <b>Highest</b> . Can be changed on the Action menu.
Request Date	When the file upload was requested.
Requester	The console user that requested the upload, or “System” if the request was due to an event rule.
Status	<p>The status of the file upload. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Uploaded</b> – The upload completed successfully and the file is available on the server.</li> <li>• <b>Uploading</b> – The upload is in progress but not yet complete; a partial file has been received by the server. This status is likely to appear only for very large files.</li> <li>• <b>Initiated</b> – The upload task has been received by the agent where the file is located.</li> <li>• <b>Queued</b> – The upload task has not yet been sent to the agent.</li> <li>• <b>Error</b> – The upload failed. Hovering the cursor over this status displays the error message. Errors include: No file with hash, The system cannot find the path specified, The system cannot find the file specified.</li> <li>• <b>Canceled</b> – The upload was cancelled by a console user.</li> </ul>

Column	Description
Computer	The name of the computer from which the file was uploaded.
File Name	The name of the uploaded file. For most requests, the Bit9 Server uploads a file matching the <i>hash</i> of the requested file, so in some cases, the name shown here will not be the same as the name of the file you chose. For uploads from the Computer Details page, the file name is always the name entered in the File box during the upload request.
File Size	The size (in bytes) of the file.
Upload %	The percent of the upload that is finished. Completed uploads show 100%. Failed uploads and uploads not yet started show 0%.
Upload Date	When the file was uploaded to the server.
Upload Directory	The directory on the Bit9 Server to which the file was uploaded. Value is "(default)" for manual uploads, which use the directory configured in the System Configuration Advanced Options tab. If the upload is due to an event rule, the actual path is shown.
Error	A description of the error that prevented the file from uploading. For example, the error for a file that was not present at the location given (or at all) would be <b>file not found</b> . Not shown by default.
File Path	The location on the agent computer from which the file was uploaded. Not shown by default.
Prevalence	The number of Bit9-managed computers reporting to your server on which this file is present.
MD5	The MD5 hash of the file.
SHA256	The SHA-256 hash of the file.
Source	Source of the request for upload. Either "Event rule" or "Manual".
Source Name	If the request was due to an event rule, the name of the rule. If the request was manual, this field is empty.

## Diagnostic Files

The Requested Files page also has an Diagnostic Files tab that shows diagnostic files uploaded from Bit9-managed endpoints to the Bit9 Server. There are two types of diagnostic files uploadable to the server: Server Diagnostic files and Agent Diagnostic Files. Server Diagnostic Files can be downloaded to a console user's own computer by clicking the download button next to the checkbox for the file in table. Agent Diagnostic files remain on the server and do not have a download option.

The information and actions on the Diagnostic Files tab are generally used in conjunction with Bit9 Technical Support.

See [Appendix D, "Diagnostic Files,"](#) for more on uploading and downloading diagnostic files.


## Downloading Uploaded Files

Once files are uploaded to the Bit9 Server, console users with the appropriate permissions can download selected files to their local computer for further examination.

### Important

This feature in particular should be used with extreme care, and in full compliance with your organization's policy on accessing other users' files. Be sure that only those Bit9 Console users that absolutely need access to the feature are given permission to use it. The ability to download files has its own permission setting (called "Access uploaded files") in the console user permissions settings.

### To download an uploaded file:

1. In the Uploaded Files table, click on the download button  in the row for the file you want to download.
2. Follow the prompts for your browser to choose to download the file.

This copies a zip file to the download location on the computer on which the console is being viewed. The zip file includes the uploaded file and the folder path from the agent computer. You can navigate down through the folders to the file.

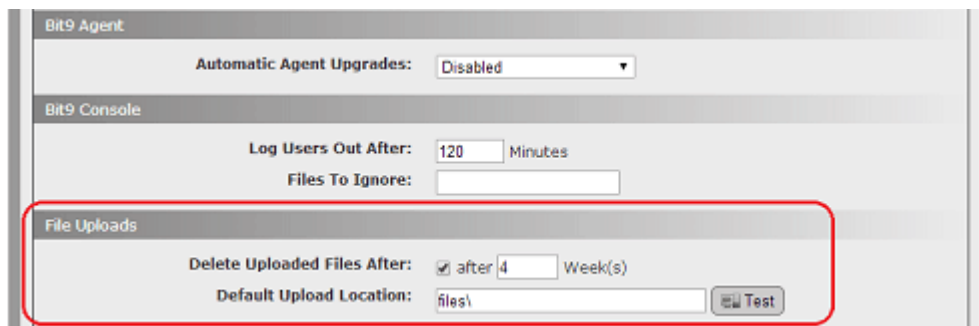
## Upload Configuration Options

### Deleting Uploaded Files

You can delete individual uploaded files from the server by checking the row for each file you want to delete on the Uploaded Files page and choosing **Delete Uploads** on the Action menu. You also can configure the Bit9 Server to delete files uploaded to the server on a schedule. By default, uploaded files are deleted after they have been on the server for 4 weeks.

### To configure automatic deletion of uploaded files:

1. On the console menu, choose **Administration > System Configuration** and then click on the **Advanced Options** tab on the System Configuration page.
2. Click the **Edit** button at the bottom of the page.



3. In the File Uploads panel, make sure the Delete Uploaded Files After box is checked, and enter the number of weeks after which you want the files to be deleted.  
**Note:** Disabling automatic deletion of uploaded files is not recommended..
4. Click the **Update** button at the bottom of the page.

#### Note

The actual uploaded files are not included in Bit9 Server backups, although the Uploaded Files table is backed up. If you restore a Bit9 database and there were files listed in the Uploaded Files table, the table is restored but the files will not be available.

## Changing the Uploaded File Location

The default location of zipped, uploaded files is in the *Parity Server\Files* folder of the Bit9 installation directory. Uploaded files are stored in numbered zip files. For example, the first file you upload might be in the following location:

```
C:\Program Files (x86)\Bit9\Parity Server\Files\1.zip
```

You can change this location if you choose by editing the Default Upload Location setting on the System Administration/Advanced Options page (see the illustration above). You can specify locations in the following ways:

- If you specify a folder without a full path, the location is assumed to be relative to the *Bit9\Parity Server\* directory on the Bit9 Server. So, for example, the default location shown above is specified on the Advanced Options page simply as *files\*.
- You can specify a full path, including a drive letter, on the Bit9 Server.
- You can use a full UNC path to specify a location on a system other than the Bit9 Server.

However you specify the upload location, you must have write permission to the location and, for UNC paths, network access to the specified system.

#### To change the target location for uploaded files:

1. On the console menu, choose **Administration > System Configuration** and then click on the **Advanced Options** tab on the System Configuration page.
2. Click the **Edit** button at the bottom of the page.
3. In the File Uploads panel, enter the path for the location to which you want uploaded files sent and click the **Test** button to make sure that the location exists.

**Note:** If you specify a directory that does not exist, clicking the Test button may produce a failure message. However, if you have permission to write in the directory above the location you identified, the folder will be created and files will be uploaded to that location.



4. Click the **Update** button at the bottom of the page.

**Note**

If you have licensed the Bit9 Connector, you also can use Event Rules to automatically upload files that match the file specifications in a rule, and can define a new location for each rule. See [“Event Rules”](#) on page 423.



## Appendix F

# Exporting Bit9 Data for External Analysis

This chapter provides instructions for configuring and using Bit9 External Analytics, which enables the Bit9 Server to export data it collects from endpoints to external analysis tools. This integration can enhance your ability to analyze Bit9 data and makes it possible for the external tool to analyze data from multiple sources, including other Bit9 Servers.

### Note

For this release, Bit9 has implemented the External Analytics integration with Splunk, and the examples shown here are Splunk-specific. However, the general description of configuration of data export as described in this appendix should enable integration with other external analysis tools by users with expertise in the setup of those tools.

### Sections

Topic	Page
<a href="#">Overview</a>	760
<a href="#">Preparing to Use External Analytics</a>	760
<a href="#">Data Format and Management</a>	761
<a href="#">Enabling External Analytics in the Bit9 Console</a>	763
<a href="#">Enabling an External Tool for Bit9 Data Analytics</a>	767
<a href="#">Enabling Splunk to Collect Bit9 Data</a>	768
<a href="#">Viewing Bit9 Data in External Analytics Tools</a>	770
<a href="#">Using the Splunk App for Bit9 Security Platform</a>	771

## Overview

The Bit9 Security Platform provides Syslog event output that can be analyzed and displayed by multiple different tools. Beginning with release v7.2, the Bit9 external analytics integration feature provides another way to utilize the extensive data collected by the Bit9 Platform. A Bit9 Server can be configured to send data to external data analytics tools, such as Splunk. Integrating Bit9 with an external analytics tool offers the following advantages:

- **Analyze Data from Multiple Sources** – You can view Bit9 information in context with streams of information from other data security platforms or multiple Bit9 Servers. For this release, Bit9 data imported to Splunk can be normalized to the CIM standard.
- **Add Bit9 File Data to Analysis** – Unlike Syslog-based integrations, the external analytics integration is not limited to *event* log output. You can choose to export Bit9 event data, the file catalog, and/or file operations data to the external tool. The type and amount of data you send is configurable in the Bit9 Console.
- **Use New Reporting Capabilities** – You can use the capabilities of an external tool to generate new types of reports from your Bit9 data.
- **Shift the Analysis Load** – You can reduce the load on the Bit9 database server by moving data analysis to another tool and location.
- **Link the Bit9 Console to External Reporting Tools** – Enabling an analytics integration can add links from certain Bit9 Console pages to the external analysis tool console.

Data exported for external analytics is in JSON format.

### Note

File Catalog data available in Bit9 is described in [Chapter 7, “File and Publisher Information.”](#) The events available from the Bit9 Platform are described in the separate *Bit9 Events Integration Guide*.

## Preparing to Use External Analytics

To use the external data analytics features, do the following:

- Configure the Bit9 Server to send data to a folder for external analytics.
- Enable one or more Bit9 Console user accounts with the privileges related to external analytics: *View System Configuration*, *Manage System Configuration*, and (to view links to and access external tools from the Bit9 Console) *View External Analytics Reports*. See [“Account Group Permissions”](#) on page 93 for more on user privileges.
- If you plan to link back to the external tool from the Bit9 Console, make sure that the Bit9 Console users who will be using the analytics integration also have login accounts on the external tool.
- Configure your analytics tool to consume the output.

## Data Format and Management

Data for external analytical tools is exported in JSON format. The JSON output from the Bit9 Server includes the field name with each value, making it easier both to view the raw output and to parse it later without creating indexing dependencies.

```
[
  {
    "MessageTime": "2014-03-25 21:56:39.891",
    "HostId": 1,
    "HostName": "MYCORP\\BIT9SERVER1",
    "HostIP": "dc60::123b:9ab8:987d:3456",
    "Bit9Server": "bit9server1.mycorp.local",
    "RequestHeader": {
      "Method": "REPORT_AB_LIST",
      "MethodVersion": 11,
      "Timestamp": "2014-03-25 21:06:49",
      "FileHash": "",
      "PathName": "c:\\windows\\microsoft.net\\framework64\\v2.0.50727\\mscorlib.exe -useclsid {701c54a0-0cdd-4eca-b729f72bf23451} -comment \\\"compile worker for microsoft.web.management.iisclient, version=7.5.0.0, culture=neutral, publickeytoken=31bf3856ad364e35, processorarchitecture=msil\\\"",
      "FileName": "c:\\windows\\microsoft.net\\framework64\\v2.0.50727\\mscorlib.exe",
      "SourcePathName": "",
      "SourceFileName": "",
      "Flags": 0,
      "ProcessPath": "c:\\windows\\microsoft.net\\framework64\\v2.0.50727\\mscorlib.exe",
      "ProcessHash": "",
      "MsiId": 0,
      "OpType": 9,
      "LocalState": 8,
      "FileHashType": 0,
      "InstallerHashType": 5,
      "ProcessHashType": -1,
      "DetachedPublisher": "",
      "TrustedDirectoryId": 0,
      "ProcessKey": "00000001-00000000-00000000-000000005331EFD9"
    },
    "UserName": "NT AUTHORITY\\SYSTEM",
    "UserSID": "",
    "InstallerHash": "654013b8fd229a50017b08dec6ca19c7dda8ce0771260e057a92625201d539b1",
    "ProcessHash": "",
    "Id": 2,
    "MsiId": 0,
    "OpType": 9,
    "LocalState": 8,
    "FileHashType": 0,
    "InstallerHashType": 5,
    "ProcessHashType": -1,
    "DetachedPublisher": "",
    "TrustedDirectoryId": 0,
    "ProcessKey": "00000001-00000000-00000000-000000005331EFD9"
  },
  {
    "MessageTime": "2014-03-25 21:56:40.300",
    "HostId": 1,
    "HostName": "MYCORP\\BIT9SERVER1",
    "HostIP": "dc60::123b:9ab8:987d:3456",
    "Bit9Server": "bit9server1.mycorp.local",
    "RequestHeader": {
      "Method": "REPORT_AB_LIST",
      "MethodVersion": 11,
      "Timestamp": "2014-03-25 21:07:40",
      "FileHash": "",
      "PathName": "c:\\windows\\microsoft.net\\framework64\\v2.0.50727\\mscorlib.exe -useclsid {63f258b3-6dd5-478f-8d2c0a36852cfe8f} -comment \\\"compile worker for microsoft.datawarehouse.vsiintegration, version=10.0.0.0 culture=neutral, publickeytoken=89849dcd8080cc91\\\"",
      "FileName": "c:\\windows\\microsoft.net\\framework64\\v2.0.50727\\mscorlib.exe",
      "SourcePathName": "",
      "SourceFileName": "",
      "Flags": 0,
      "ProcessPath": "c:\\windows\\microsoft.net\\framework64\\v2.0.50727\\mscorlib.exe",
      "ProcessHash": "",
      "MsiId": 15,
      "OpType": 9,
      "LocalState": 8,
      "FileHashType": 0,
      "InstallerHashType": 5,
      "ProcessHashType": -1,
      "DetachedPublisher": "",
      "TrustedDirectoryId": 0,
      "ProcessKey": "00000001-00000000-00000000-000000005331F01B"
    },
    "UserName": "NT AUTHORITY\\SYSTEM",
    "UserSID": "",
    "InstallerHash": "39d3630e623da25b8444b6d3aaab16b98e7c289c5619e19a85d47b74c71449f3",
    "ProcessHash": "",
    "Id": 15,
    "MsiId": 0,
    "OpType": 9,
    "LocalState": 8,
    "FileHashType": 0,
    "InstallerHashType": 5,
    "ProcessHashType": -1,
    "DetachedPublisher": "",
    "TrustedDirectoryId": 0,
    "ProcessKey": "00000001-00000000-00000000-000000005331F01B"
  }
]
```

If you are using the Splunk App for Bit9 Security Platform, Bit9 data imported by the Splunk Server is mapped to the CIM so that it can be integrated with other data. See [“Field Mappings to CIM in the Splunk App for Bit9”](#) on page 777 for details.

Depending upon which messages you enabled for export, one or more of the following files will appear in the Export Directory configured for External Analytics:

- **Event Data** – EventTrace-<YYYYMMDD>.bt9
- **File Catalog Data** – MetadataTrace-<YYYYMMDD>.bt9
- **File Operations Data** – NetTrace-<YYYYMMDD-HHMMSS>.bt9

Name	Date modified	Type	Size
EventTrace-20140325.bt9	3/25/2014 2:45 PM	BT9 File	2,060 KB
MetadataTrace-20140325.bt9	3/31/2014 7:47 AM	BT9 File	16,575 KB
NetTrace-20140325-145639.bt9	3/29/2014 1:52 PM	BT9 File	52 KB

Each message log file will grow to a maximum of 512 megabytes, at which point a new log file will be created. New logs are also started when the Bit9 Server processes are restarted.

New File Operations data files (NetTrace) are named with both date and time as described above.

If two Event data or File Catalog data files are created on the same day, a number is appended to the second one of each. For example, the first file catalog data file created on October 29, 2013, would be named *MetadataTrace-20131029.bt9*. If that file reached its size limit that same day, the second file would be named *MetadataTrace20131029-1.bt9*.

#### Note

See the separate *Bit9 Event Integration Guide* for more information about event types and subtypes that may be exported.

## Data Volume for Exported Analytics

- 20KB per computer per day of file catalog
- 75KB per computer per day of events
- 135KB per computer per day of file operations (volume: High)
- 115KB per computer per day of file operations (volume: Medium)
- 100KB per computer per day of file operations (volume: Low)

## Limiting Export Directory Size

There is a checkbox on the console External Analytics tab of the System Configuration page that allows you to limit the amount of data in the Export Directory. Checking this box displays a field in which you can enter the number of gigabytes of data to set as the maximum export directory size (i.e., the total size of all files in the Export Directory). When the limit is reached, files are deleted by age (oldest first) until the directory size is under the limit. The lowest allowable size limit is 3 GB. The current files in each category are never deleted. The upper limit is 10 petabytes.

#### Note

The Export Directory size limit controls the amount of data kept in the directory on the Bit9 Server but does not limit the amount of data uploaded to the external analysis tool. If you need to limit the data going to the external tool for licensing or performance reasons, use the External Analytics Settings checkboxes and radio buttons on the External Analytics configuration page, as described in [“Enabling External Analytics in the Bit9 Console”](#) on page 763.

## Local vs. Network Log Files

When log files are local and the log content is relayed to the data analytics tool by a mechanism designed for that purpose, such as the Splunk Universal Forwarder, there should be minimal performance impact. However, if log files are written to a network location, there could be a delay in data availability if the network latency is high.

When analytics data is written locally, it should be written to a disk other than the one on which the operating system or Bit9 SQL database are located.

## Enabling External Analytics in the Bit9 Console

You configure three elements of the Bit9 analytics features in the Bit9 Console:

- On the System Configuration page External Analytics tab, you specify the location, content, and size limitation (if any) for folder into which Bit9 data is exported.
- On the same tab, you can provide URLs and query specifications so that Bit9 Console users can link to specific reports on an external analytics server.
- On the Add Custom Rule page, you can create a rule that will ignore files written to the data export directory to reduce the impact of data exports on the Bit9 Server.

The following procedure describes how to accomplish the first two tasks on this list. [Table 129, “External Analytics Configuration Options”](#) on page 765 provides more detail on the parameters on the External Analytics tab.

### To enable External Analytics features in the Bit9 Console:

1. On the console menu, choose **Administration > System Configuration** and click on the **External Analytics** tab.
2. Click the **Edit** button at the bottom of the page.

3. In the General panel, check the **Enable Export** box.

4. In the Export Directory field, enter the name of the directory into which you want Bit9 analytics files written. This folder must be one for which the user running the Bit9 Server service (*ParityServer*) has write access.

**Note:** If you plan to write exported data to the system that is hosting the Bit9 Server, you should use a disk volume other than those used by the operating system or SQL Server.

5. Click the **Test** button to the right of the Export Directory field to test whether the directory is valid and the server process has write access to it.
6. In the Messages fields, specify what type of information you want to export:

- a. **File Catalog** – Check this box to export File Catalog data to the export directory. Checking the box displays two radio buttons: **Export complete catalog** exports the entire current contents of the File Catalog and any new additions to the catalog. **Export only new files** exports only unique, new files discovered on agents reporting to your Bit9 Server once this option has been enabled.
- b. **File Operations** – Check this box to export messages from agents about operations that affect files. A dropdown menu lets you determine the volume, and by extension the type, of the data that is exported. See [Table 129](#) for details.
- c. **Events** – Check this to export Bit9 events. See [Table 129](#) for details about the radio button options that control the amount of Event data that is exported and display the estimated size of the export where available.

### Note

When setting these Message export options, consider the traffic estimate values shown for each one and any traffic limits on the external analysis device. However, you should also be sure you are exporting enough data to allow for useful analysis.

7. The Analytics Server Reports section allows configuration of links from the Bit9 Console to reports on the external analytics server. If you want to enable these links, begin in the Root URL field, by entering the root URL of the analytics tool with which you are integrating the Bit9 Platform.
8. In the Analytics Server Reports panel, enter and test the Relative URL and Query string for each type of report listed. Use the marker **<va1>** in the query string to represent what is being passed (file hash, machine name, user name) to the analytics tool.
9. Click **Update**.



**Table 129:** External Analytics Configuration Options

Field/Button	Description
<b>Enable Export</b>	This checkbox activates and deactivates the Bit9-External Analytics integration features, including data export and links to external analytics tools.
<b>Export Directory</b>	This field determines the directory to which the Bit9 Server exports data for external analysis. The Test button allows you to confirm that the directory is valid and that the server process has write access to it. The test results appear next to the button (either 'OK' for success or a message explaining why the test failed).
<b>Messages: File Catalog</b>	This checkbox enables export of File Catalog data to the export directory. Checking the box displays two radio buttons that control the amount of File Catalog data that is exported: <ul style="list-style-type: none"> <li>• <b>Export complete catalog</b> – This option exports the entire current contents of the File Catalog and continues exporting any new additions to the catalog.</li> <li>• <b>Export only new files</b> – This option exports only unique, new files discovered on agents reporting to your Bit9 Server.</li> </ul>
<b>Messages: File Operations</b>	This checkbox enables export of messages from agents about operations that affect files. A dropdown menu lets you determine the volume, and by extension the type, of data that is exported: <ul style="list-style-type: none"> <li>• <b>Low</b> – Export messages about file Create, Modify, Delete, Rename, and Rename Directory operations.</li> <li>• <b>Medium</b> – Export all messages in Low plus messages about file state changes (Approved, Unapproved, Banned); this includes both individual file state changes and operations that cause state changes in groups of files.</li> <li>• <b>High</b> – Export all file operations messages.</li> </ul>
<b>Messages: Events</b>	This checkbox enables export of Bit9 events data. Checking the box displays radio buttons that control the amount of Event data that is exported, and displays the estimated size of the export where available: <ul style="list-style-type: none"> <li>• <b>Include entire event backlog (est. value KB) plus new events</b> – This exports the entire existing event database and enables ongoing export of new events.</li> <li>• <b>Include event backlog going back [time value] (est. value KB) plus new events</b> – This allows you to choose a time period of past events (starting from the present) to export and enables ongoing export of new events beginning when this is enabled.</li> <li>• <b>New events only</b> – This enables ongoing export of new events only beginning when this setting is enabled.</li> </ul>
<b>Limit Export Directory Size</b>	Checking this box displays a field in which you can enter the number of gigabytes of data to set as the maximum export directory size (i.e, the total size of all files in the Export Directory). When the limit is reached, files are deleted by age (oldest first) until the directory size is under the limit. The lowest allowable size limit is 3 GB. The current files in each category are never deleted.

Field/Button	Description
<b>Root URL</b>	<p>The root URL (optionally including the port) entered here points to the analytics server with which you are integrating the Bit9 Server. This is used as the base URL for links from Bit9 Console pages back to reports on the analytics server.</p> <p><b>Note:</b> The Bit9 Console user must have credentials to log into the external server, and the URL provided must allow the user to log in with those credentials, even when using the Bit9 Console to reach it.</p>
<b>File Details Report</b>	<p>This defines a link to a File Investigation report on the analytics server. There are two fields to define the line: Relative URL, which is appended to the Root URL you define, and Query String, which defines the report you want from that URL.</p> <p>When defined, this <b>File Analytics</b> link appears in the External Pages menu on the File Details and File Instance Details pages.</p> <p>Click the <b>Test</b> button to the right of this line to confirm that the URL and query definition are valid.</p>
<b>Computer Details Report</b>	<p>This defines a link to a Computer Investigations report on the analytics server. There are two fields to define the line: Relative URL, which is appended to the Root URL you define, and Query String, which defines the report you want from that URL.</p> <p>When defined, this <b>Computer Analytics</b> link appears in the External Pages menu on the Computer Details page.</p> <p>Click the <b>Test</b> button to the right of this line to confirm that the URL and query definition are valid.</p>
<b>User Details Report</b>	<p>This defines a link to a Console User Search (in this case, Bit9 Console Login Accounts) report on the analytics server. There are two fields to define the line: Relative URL, which is appended to the Root URL you define, and Query String, which defines the report you want from that URL.</p> <p>When defined, this <b>User Analytics</b> link appears in the External Pages menu on the Edit Login Account page.</p> <p>Click the <b>Test</b> button to the right of this line to confirm that the URL and query definition are valid.</p>
<b>Set Analytics URLs to Splunk defaults</b>	<p>Clicking this button inserts Splunk default Relative URL and Query String definitions into the three report fields. It also inserts "http://server:8000" in the Root URL field (port 8000 is the Splunk default).</p> <p>When you replace "server" with a valid Splunk server URL, these defaults should allow access to valid Splunk reports from the Bit9 Console.</p>
<b>Clear Analytics URLs</b>	<p>Clicking this button clears all values from the Analytics Server and Analytics Server Reports fields.</p>

## Editing or Disabling the External Analytics Integration

If you need to modify or disable the external analytics integration with the Bit9 Server, you can use the External Analytics tab on the System Configuration page in the Bit9 Console. The Export Directory and any additional components installed for an integration, such as the Splunk Universal Forwarder, are not deleted or uninstalled when you disable the integration through the Bit9 Console.

## Adding a Custom Rule to Ignore Analytics Log Files

When External Analytics is enabled, there will be repeated, ongoing file write operations in the Export Directory. Normally, this would generate significant event traffic on the Bit9 Server if an agent is active on the server. Since this event traffic should not be interesting to track, consider creating a custom rule to exclude tracking of files in the Export Directory. See [Chapter 12, “Custom Software Rules,”](#) for more about how these rules may be configured.

### To exclude tracking of exported analytics files:

1. On the console menu, choose **Rules > Software Rules** and click on the **Custom** tab.
2. Click the **Add Custom Rule** button.
3. On the Add Custom Rule page, provide the necessary information to create a rule that will ignore writes to the Export Directory for analytics data:
  - a. **Name** – Choose a name to clearly identify the rule; for example, *Ignore Data Analytics Log Files*.
  - b. **Description** – (Optional) Add a description to further identify the rule purpose.
  - c. **Status** – Click the **Enabled** radio button.
  - d. **Platform** – Choose the platform to which the rule is applied; this is **Windows** (the default) for Export Directories that are on the Bit9 Server system.
  - e. **Rule Type** – Choose **Performance Optimization**.
  - f. **Path or File** – Provide the Path and Name of the folder where analytics files are written; for example, `D:\Bit9Analytics`.
  - g. **Process** – Choose **Specific Process**, then enter and **Add** the processes that Bit9 uses to write these files. For example, if you are running a 64-bit OS and used the default Bit9 installation directory, you would use:
 

```
<ProgramFiles>\Bit9\Parity Server\ParityServer.exe
<ProgramFiles>\Bit9\Parity Server\Reporter\ParityReporter.exe
```
  - h. **Rule Applies To** – Choose **All policies** or if you prefer just the policy that the system being written to (usually the Bit9 Server) belongs to.
4. When you have finished configuring the rule, click the **Save** button. The new rule is added to the Custom Rules table.

## Enabling an External Tool for Bit9 Data Analytics

In addition to configuring the Bit9 Server to export data and (optionally) connect to an analytics server for reports, you must configure a connection for the analytics server to access the exported Bit9 data. The exact steps for enabling a particular external tool for Bit9 data access will vary, and can include actions taken on the Bit9 Server system as well as those taken on the analytics server. The next section provides the steps for enabling Splunk for Bit9 data access.

## Enabling Splunk to Collect Bit9 Data

To enable a Splunk server to import Bit9 data for analysis, you must make modifications on both the system hosting the Bit9 Server and the Splunk server. The summary of these steps is as follows:

- Have a Splunk Server running and network-accessible to the Bit9 Server.
- Set up the Splunk Server to receive messages from the Splunk Forwarder.
- Install the Splunk App for Bit9 Security Platform on the Splunk Server.
- Install the Splunk App for Bit9 Security Platform on any machines running Splunk Indexer that are not on the machine running Splunkweb.
- Install the Splunk forwarder on the Bit9 server.
- Install the Splunk App for Bit9 Security Platform on the Splunk Forwarder.

## Configuring the Splunk Server for Bit9 Access

You must complete several procedures on the Splunk Server to enable use of Bit9 data for analytics. First, configure the Splunk Server to receive forwarder data on port 9997.

### To set up the Splunk server to receive Splunk Universal Forwarder messages:

1. Log into the Splunk server as an administrator-level user.
2. In the menu bar at the top of the Splunk console, choose **Settings** (Splunk 6) or **Management** (Splunk 5), then choose **> Data > Forwarding and receiving**, and in the *Forwarding and receiving* window, choose **Configure receiving**.
3. In the *Receive data* window, check to see whether port 9997 is configured. If not, click the **New** button, enter **9997** as the port to listen on, and click the **Save** button.
4. In your firewall, create a rule to ensure that the Splunk Server can receive data on port 9997.

The Splunk App for Bit9 Security Platform allows Splunk to interpret data provided by Bit9 so that it can be analyzed and displayed by Splunk.

### To install the Splunk App for Bit9 Security Platform on the Splunk Server:

1. Log into the Splunk server as an administrator-level user.
2. Search for “Bit9” through the **Find Apps Online** feature in the Splunk console, and when you find the Splunk App for Bit9 Security Platform, download it to a convenient location on the server.
3. In the menu bar at the top of the Splunk console, choose **Apps > Manage Apps**.
4. Install the App from its zip file:
  - Click on **Install app from file** and in the *Upload an app* dialog, browse to the `bit9-security-platform_10.tgz` file. and then click **Upload**. Note that the numbers at the end of the file name may vary with version changes.

**Note**

If you have Splunk indexers that are not on the machine running the Splunkweb, you should also install the Splunk App for Bit9 Security Platform on the machines hosting these indexers. The procedure for this is the same as for installing the app on the Splunk Forwarder. See “[To install the Splunk App for Bit9 Security Platform on the Bit9 Server:](#)” on page 769

**Installing the Splunk Forwarder and App on the Bit9 Server**

In addition to configuring External Analytics on the Bit9 Console, there are two additional steps you must take on the system hosting the Bit9 Server, outside the console itself, to enable Splunk connectivity:

- Install the Splunk Universal Forwarder
- Install the Splunk App for Bit9 Security Platform in a Forwarder subdirectory

The Splunk Universal Forwarder is a package that can be installed on systems so that Splunk can collect data from them, for example from log files. In this case, when the Forwarder and Splunk App for Bit9 are installed, the Forwarder collects data from the Bit9 export folder and directs it to the correct location in the Splunk infrastructure.

**Important**

During the Splunk Universal Forwarder installation process, *do not* enter the location of the data files on the Bit9 Server when prompted. The location of these files will be provided by the Splunk App for Bit9 Security Platform.

**To install the Splunk Forwarder on the Bit9 Server:**

1. Download the forwarder from the Splunk website:  
<http://www.splunk.com/download/universalforwarder>
2. Run the appropriate installer for your operating system on the Bit9 Server.
3. Provide the address of your Splunk Server when prompted.
4. Once the Splunk Forwarder is installed, install the Splunk App for Bit9 Security Platform under the Splunk Forwarder installation directory, as instructed below.

**To install the Splunk App for Bit9 Security Platform on the Bit9 Server:**

1. Search for and download the Splunk App for Bit9 Security Platform from the Splunk apps website:  
<http://apps.splunk.com>
2. Copy the downloaded file, for example, `bit9-security-platform_10.tgz`, to the `\etc\apps` subdirectory under the Splunk Forwarder installation directory. For example, if you are running a 64-bit OS on the Bit9 Server copy the file to:  
`C:\Program Files\SplunkUniversalForwarder\etc\apps\`

**Note:** The numbers at the end of the file name may vary with app version changes.

3. Unzip and untar the file.
4. Go into the `TA-bit9` directory and create a new directory named `local`.
5. Copy `default\inputs.conf` into the `local` directory.
6. Edit the first line of `local\inputs.conf` to point to the location of the Export Directory configured on the Bit9 console System Configuration/External Analytics page, and save the file. For example, if the Export Directory on the Bit9 Server is `D:\Bit9\LogFiles`, the first line of `inputs.conf` should be changed to the following:

```
[monitor://D:\Bit9\LogFiles\*.bt9]
```

7. At a command prompt, restart the Splunk Forwarder:

```
cd \Program Files\SplunkUniversalForwarder\bin
.\splunk.exe restart
```

When you have completed all of the tasks described in “[Enabling External Analytics in the Bit9 Console](#)” and “[Enabling an External Tool for Bit9 Data Analytics](#)”, the Bit9-Splunk integration should be complete and data from Bit9 should begin flowing to Splunk.

## Viewing Bit9 Data in External Analytics Tools

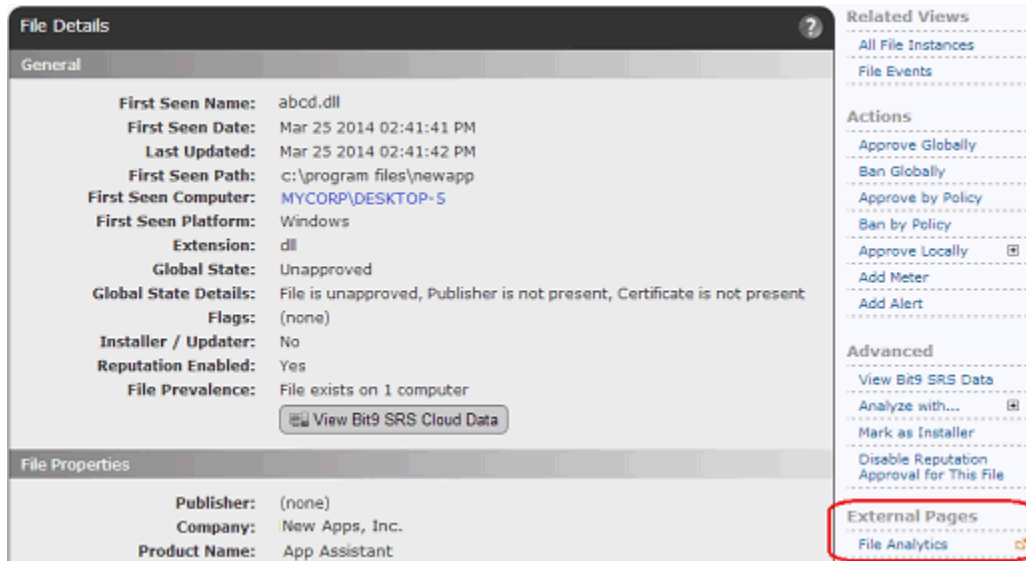
How an external analytics tool uses Bit9 data will vary according to the reporting capabilities of the tool and its ability to integrate Bit9 information with streams of information from other data security platforms. Users of this integration are assumed to have knowledge of how to integrate data from various sources in their analytics tool, and how to create reports that make use of that information. The specific reports that are created are up to each user.

One way to make use of reports on an external analytics tool is to link to them from the Bit9 Console.

### Linking to an External Tool from the Bit9 Console

The External Analytics tab of the Bit9 Console System Configuration page provides fields in which links to reports on an external tool may be defined. If a Root URL and Analytics Reports for each category are configured on this page, the following links appear in the right menu of their respective pages:

- **Computer Analytics** – This appears on the Computer Details page.
- **File Analytics** – This appears on the File Details and File Instance Details pages.
- **User Analytics** – This appears on the Edit Login Account page.



The content of the pages displayed when a Bit9 Console user clicks one of these links is completely determined only by the URL and query definitions provided on the configuration page. The Bit9 Console user must have credentials to log into the external server, and the URL provided must allow the user to log in with those credentials even when using the Bit9 Console to reach it.

See “[Enabling External Analytics in the Bit9 Console](#)” on page 763 for details of how these links are enabled. See “[Using the Splunk App for Bit9 Security Platform](#)” for an example of what these reports might contain.

## Using the Splunk App for Bit9 Security Platform

The *Splunk App for Bit9 Security Platform* helps Splunk present Bit9 data more effectively. Installing and configuring the app adds a set of dashboards specifically for displaying Bit9 data. It also enhances Splunk’s ability to handle Bit9 data in other views, for example, by identifying Bit9 as the source of the data, identifying the purpose of each keyword in the key/value pairs, decoding Bit9-specific values, and by mapping Bit9 fields to the Common Information Model (CIM) so that Bit9 data can be combined with data from other sources.

### Dashboards in the Splunk App for Bit9

The Splunk App for Bit9 Security Platform includes the following dashboards:

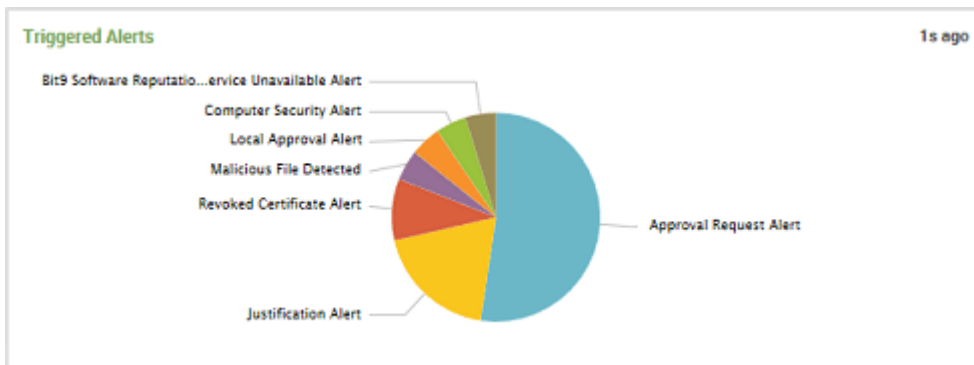
- **Deployment Activity** – Overview of information available from the Bit9 Platform installation.
- **Activity Details: File Activity** – Information about file creation and modification activity on Bit9-managed computers.
- **Activity Details: Blocks** – Information about files blocked on Bit9-managed computers.
- **Activity Details: Approvals** – Information about files approved on Bit9-managed computers.



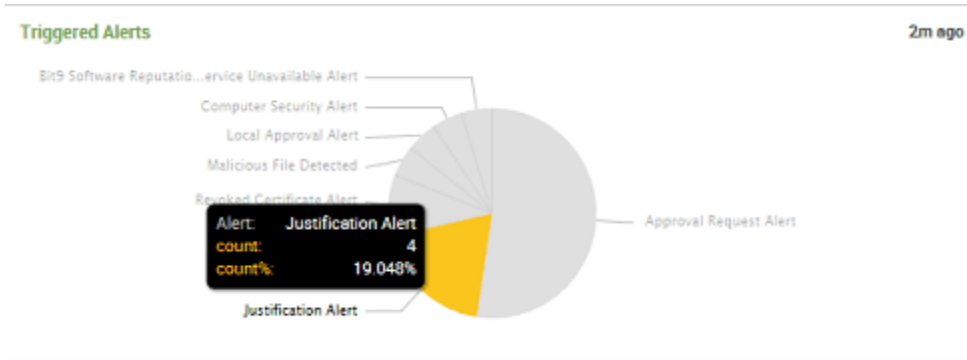
- **Activity Details: New Unapproved Files** – Information about new files that are discovered on Bit9-managed computers and neither approved nor banned.
- **Activity Details: Events** – Information about events recorded on the Bit9 Server.
- **File Investigation** – Information suitable for a malware investigation focused on a specific file or files. If you link from the Bit9 Console, this provides information about the file from whose details page you linked.
- **Computer Investigation** – Information suitable for a malware investigation focused on a specific computer or computers. If you link from the Bit9 Console, this provides information about the computer from whose details page you linked.
- **Console Users** – Information suitable for discovering anomalous or risky actions performed by a specific Bit9 console user or users. If you link from the Bit9 Console, this provides information about the user from whose details page you linked.
- **All Console Users** – Information about all Bit9 Console users.

Each of these dashboards contains panels that display information imported into Splunk from a Bit9 Server. Some also include a summary panel at the top. If you have used the Dashboard in the Bit9 Console, some of these panels will be familiar. However, here they can take advantage of the analysis and multi-source integration capabilities of Splunk. [Table 130](#) shows the panels available on the Splunk App for Bit9 dashboards, and identifies the dashboards on which they appear.

Panels in these dashboards may include tables of data or charts that graphically display the data, such as the display of Triggered Bit9 Alerts in the following example. Some panels include both.



When you hover the mouse over a section of the chart, such as a pie chart slice or a bar in a bar chart, a legend appears describing the data represented that section.





If you click on one of these sections, the underlying data is displayed.

The screenshot displays the Splunk interface for event analysis. At the top, there are tabs for 'Events (4)', 'Statistics', and 'Visualization'. Below these are controls for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. A timeline visualization shows three green bars representing events. Below the timeline, there are controls for 'List', 'Format', and '20 Per Page'. On the left, there are sections for 'Selected Fields' (host 1, source 2, sourcetype 1) and 'Interesting Fields' (ABId 1, ABState 1). The main event view shows the following details:

Time	Event
3/10/14 1:54:55.000 PM	<pre> {[-]   ABId:   ABState:   BanName:   Bit9Server: IT-Server-2   CLVersion:   EventParam1: Justification Alert: 1 justification has been created.   EventParam2:   EventParam3:   EventSubType: Alert triggered   EventSubTypeId: 1104 </pre>

These panels provide other standard Splunk features, such as the ability to change the time period for which data is displayed.

**Table 130:** Panels in Splunk App for Bit9 Dashboards

Dashboard	Panel	Description
Deployment Activity	Host Activity	File and event activity by agent computer.
	Triggered Alerts	Number of triggered alerts by type.
	File Blocks	Blocked files by date, computer, and product name.
	New Unapproved Files	Events reporting new unapproved files appearing on agent computers by date.
	New Files in Catalog	Unique new files added to the catalog by date.
	Approvals	File approvals by date, computer, and product name.
	File Activity	Creation and modification of files on Bit9-managed systems by date, computer, and product or file name.
	Top Event Subtypes	Event subtypes listed by frequency.
Activity Details: File Activity	File Creations	File creations by date, computer, product or file name, and process.
	File Modifications	File modifications by date, computer, product or file name, and process.
Activity Details: Blocks	Blocks	File blocks by date, computer, and file name.
	Block Distributions	File blocks by file trust level, process that attempted to execute the file, and product name.
	Block Sources	File blocks by rule that blocked the action, reason (event subtype), and publisher.
Activity Details: Approvals	Approvals	File approvals by date, computer, and file name.
	Approval Distribution	File approvals by file trust level, process that generated, modified or executed the file, and product name.
	Approval Sources	File approvals by rule that approved the file, reason (event subtype), and publisher.
Activity Details: New Unapproved Files	New Unapproved Files	New unapproved files appearing on agent computers by date.
	New Unapproved Files By Product Name	New unapproved files listed by publisher

Dashboard	Panel	Description
Activity Details: New Unapproved Files (continued)	Top New Unapproved File Hashes	New unapproved files listed by hash, ranked from most to least instances
	Top New Unapproved File Names	New unapproved files listed by name, ranked from most to least instances.
	Potentially Malicious Files	New unapproved files identified as potentially malicious by Bit9 SRS.
	Top Computers	Computers with new unapproved files, ranked from most to least instances.
	Known Trust Values	New unapproved files listed by Bit9 SRS trust values (if known).
	Top Users	New unapproved files listed by users, ranked from most files to least files.
Activity Details: Events	Events	Events by date.
	Top Event Subtypes	Events by event subtype, ranked from most to least instances.
	Errors	Error messages.
	Top Computers	Events by agent computer referenced in event, ranked from most to least instances.
	Top Users	Events by users referenced in event, ranked from most to least instances.
	Top Event Types	Event by event type, most to least. Event types include multiple subtypes.
File Investigation	Number of computers on which this file has been created	The prevalence of this file on Bit9-managed computers reporting to this server.
	File Hashes	For file searches by name, the hashes identified for files with this name.
	File Information: First Seen on Network	The first seen name of this file on Bit9-managed computers reporting to this server.
	Hash Activity	A time-based bar chart describing creations and modifications of and by files with this hash.
	Other Hashes with First Seen Name	Other hashes with the same first seen file name on Bit9-managed computers reporting to this server.
	Files Modified By This File	Files for which this file is the process, presented as a simple table of events in reverse-chronological order

Dashboard	Panel	Description
File Investigation (continued)	Top Hashes Modified by This File	Files for which this file is the process, sorted by the number of times a particular file (identified by hash) was modified by the specified file/hash
	Top Event Subtypes Containing This File	Event subtypes containing a reference to this file, ordered from subtypes containing the most instances of this file most to least.
	Top Rules Containing This File	Rules referencing this file, including those identifying its file/hash as the process, the installer, or the file being acted upon. The rules appear in descending order by how often they reference the specified file.
Computer Investigation	Detection Events	Table of events related to Bit9 advanced threat indicators.
	Risky Behavior	Table of events related to issues with tamper protection, or the detection of potentially risky or malicious files on an agent computer.
	Risky Behavior Timeline	Amount of Risky Behavior graphed over time.
	Blocks	Chart of blocked file actions on this computer by date.
	New Files	Table of new files on the computer(s) specified in the search.
	File Activity	Chart of file creations and modifications by date.
	Approved Files	Table of files approved and the rule used for the approval.
	Events Chart	Chart of the top 10 most frequent event subtypes involving the specified computer(s) over the search time period.
	Health Checks	Table of Bit9 Health Check events and the results of the Health Check.
Console User Search	Events	Events that reference this user, charted by date.
	User Activity	Events that reference this user, in a table with additional detail, listed in date order.
	New or Removed Console Users	Console users that were created or deleted by this user.
	Custom Rules Actions	Creation and modification of custom rules by this user.

Dashboard	Panel	Description
Console User Search (continued)	File Approvals	File approvals by this user.
	File Bans	File bans by this user.
	Policy Management by Subtype	Policy management actions taken by this user, including policy modification and creation, and writing of agent installer files due to policy actions.
	Global Approval by Trust	Global approvals by the user, by trust.
	Globally Approved Hashes	Hashes globally approved by this user.
	Local Approval by Trust	Local approval by this user, by trust.
	Top Locally Approved Hashes	Files (by hash) locally approved by this user, most to least.
All Console Users	Events	Events by all console users, charted by date.
	Policy Management	Policy management events by date and user.
	Computer Management	Computer management events by date and user.
	Session and General Management	Session and General management events by date and user.
	Top Ten User - Global Approvals	Top ten users creating the most global file approvals.
	Top Ten User - Local Approvals	Top ten users creating the most local file approvals.

## Field Mappings to CIM in the Splunk App for Bit9

The Splunk Security Tool requires that data is normalized so that it can be processed and analyzed the same way, regardless of the source. The Splunk App for Bit9 Security Platform maps the fields in Bit9 data analytics output to the Common Information Model (CIM). See <http://www.dmtf.org/standards/cim> for more information on the Common Information Model.

Table 131 shows the CIM mappings done in the Splunk App for Bit9.

**Table 131:** Bit9 Data-to-CIM Mappings in Splunk

Bit9 Field	CIM Field
HostName	src_nt_host, dest_nt_host, dest, dvc_nt_host
HostIP	src_ip, dest_ip, dvc_ip
FilePath	file_path
FileHash	file_hash, hash
FileName	file_name
FileSize	file_size, size
Message	change_type
EventSubType	action
Timestamp	modtime

# Index

## A

- acknowledging
  - devices 322, 323
  - files 209
  - publishers 236, 240
- Active Directory Integration
  - AD computer metadata in Bit9 137
  - AD logins in Bit9 Console 77
  - AD policy mapping 103
  - AD user details in Bit9 Console 82
  - and agent installation 112
  - and Windows 2000 domain controllers 614
  - clearing the AD server cache 111
  - moving computers to another policy 143
  - overview 40
  - security domain for Bit9 logins 614
  - testing 104
- AD logins in console
  - disabling 79
  - enabling 77
- AD policy mapping rules 104
- administrators, Bit9 84
- Agent Disabled mode. See disabled mode agent, Bit9. See Bit9 Agent.
- alerts 494
  - alert history 510
  - alerts page 494
  - approval request 496
  - baseline drift 498
  - Bit9 SRS unavailable 496
  - blocked file 498
  - computer in local approval 495
  - computer security 496
  - configuring e-mail 635
  - creating 498
  - deleting 505
  - disabling 504
  - editing 504
  - event alerts 498
  - file prevalence 498
  - for threat detection 562
  - how triggered 505
  - justification 496
  - new certificate 303
  - on home page 51
  - propagating file 498
  - resetting 507
  - revoked certificate 303
  - types 498
  - updater modified 496
- Alerts page 495, 499, 544
- algorithms for certificates 245
- analysis environment
  - for WildFire notifications 724
- analytics
  - exporting data for 759
- analyze file
  - in Bit9 SRS 645
  - on Approval Request Details page 477
- analyzing files
  - automating with event rules 423
  - using Check Point for 734
  - using FireEye for 734
  - using WildFire for 734
- anti-virus software
  - and Bit9 Agent (Linux) 118
  - and Bit9 Agent (Mac/OS X) 117
  - and Bit9 Agent (Windows) 115
  - enabling updaters for 246
- Applications by Publisher/Company view 194
- applications. See files.
- approval mode 129
- approval requests
  - alert for 496
  - analyzing 471, 477
  - automatic resolution email 473
  - customizing the notifier interface 479
  - enabling in Windows 468
  - how users submit 469
  - in blocked file notifiers 467
  - request details page 476
  - responding to 470
  - viewing in Bit9 Console 470
- approvals
  - adding (by file) 269
  - by policy 274
  - custom 274
  - defined 224

- local 252
- removing 271
- approve on Enforcement Level transition (policy setting) 160
- approved (local state detail) 219
- approved as installer (local state detail) 219
- approved as top-level installer (local state details) 219
- Approved Files view 194
- approved not persisted (local state detail) 219
- approving devices 320
- approving files
  - automating using event rules 423
  - by automatic updaters 246
  - by custom rule 344
  - by file reputation 281
  - by hash 276
  - by importing a hash list 277
  - by local approval mode 258
  - by local approval on Enforcement Level change 253
  - by publisher approval (manual) 236
  - by publisher reputation 281
  - by trusted directory 228
  - by trusted user or group 234
  - from a deployment server 228
  - overview 224
  - printer driver updates 248
  - removing approvals 271
  - removing local approval 256
- approving publishers
  - by reputation 285
  - manual 236
- archives
  - event 493
  - in trusted directories 229
- ArcSight integration
  - specifying CEF as Syslog format 623

## B

- backups
  - backup missed alerts 495
  - Bit9 database 631
  - restoring from 634
- banned by hash (local state detail) 219

- Banned Files view 194
- banned state 218
- banning files
  - automating using event rules 423
  - by hash 227, 276
  - by importing a hash list 277
  - by name 227
  - by policy 269, 274
  - by publisher 237
  - from the Software Rules page 269
  - overview 42, 226
  - removing bans 271
- banning publishers 237
- banned by hash report-only (local state detail) 219
- bans
  - creating 226
  - custom 274
  - file name 43, 227
  - hash 43, 227
  - removing 271
  - report only 219, 227, 274
  - terminating banned processes 279
  - verifying before deployment 268
- baseline drift 521
  - adding results to a snapshot 531
  - alert for 498
  - by file category 526
  - creating and editing reports 532
  - displaying in dashboards 542
  - remediation of 530
  - snapshots for 539
  - viewing report results 525
  - viewing the list of reports 524
- Bit9 Agent
  - blocked file notifiers on 441
  - computer configuration 100
  - connection status 134
  - defined 6, 40
  - diagnostic files for 741, 754
  - disabling 153, 167
  - downloading installers for 112
  - enabling automatic upgrade 121
  - enabling management privileges 615
  - file initialization for 100
  - health check for 139
  - installing 113



- installing on Linux computers 117
- installing on Mac computers 116
- installing on Windows computers 114
- manual upgrade on Linux computers 125
- manual upgrade on Mac computers 124
- manual upgrade on Windows computers 122
- policy status of 130
- prioritizing updates to 140
- registration with server 111
- reporting command lines on 492
- requesting update for 140
- rules out of date for 130
- securing communications with 623
- self-protection 159
- temporary policy override for 262
- uninstalling 127
- uninstalling from a Mac computer 128
- uninstalling from a Windows computer 127
- uninstalling on Linux computers 128
- upgrade status 125
- upgrading 119
- upgrading by policy 155
- upgrading from console 121
- using anti-virus software with (Mac/OS X) 117
- using anti-virus software with (Windows) 115
- using with anti-virus software (Linux) 118
- verifying installation 119
- Bit9 Connector 687
  - console account permissions for 718
  - enabling Check Point integration 698
  - enabling FireEye integration 709
  - enabling Palo Alto Networks integration 692
- Bit9 Console
  - browser certificate for 48
  - creating accounts 76
  - default starting page 71
  - defined 6
  - Home page 53
  - logging in 48
  - logging out 49
  - using 47
- Bit9 Console menu bar 53
- Bit9 database. See database, Bit9
- Bit9 Server
  - defined 6, 40
  - installing. See Installing Bit9 Server guide
  - overview 34
  - restoring 634
  - status information 612
  - version number 49
- Bit9 Software Reputation Service
  - alert when unavailable 496
  - defined 40
  - enabling and disabling 643
  - file category 207
  - file category information from 194
  - file trust rating 40, 207
  - proxy settings 643
  - synchronization with 647
  - threat level 207
  - using a proxy server 646
- Bit9 SRS. See Bit9 Software Reputation Service
- block banned file hashes (policy setting) 159
- block banned file names (policy setting) 158
- block files with banned publishers or certificates (policy setting) 159
- block network executables (policy setting) 159
- block unanalyzed scripts and executables (policy setting) 158
- block unapproved executables (policy setting) 158
- block unapproved scripts (policy setting) 158
- block-and-ask. See Medium Enforcement Level
- blocked file notifiers. See notifiers
- blocking files 167
  - by custom rule 336
  - by file ban 226
  - by publisher 237
  - by script rule 376
  - on devices 316
- browsers
  - certificates warnings in 48
  - supported 48

- BSX files
  - for manual Linux agent upgrades 125
  - for manual Mac agent upgrades 124

## C

- cache, AD
  - clearing 111
- Carbon Black
  - and Computer Details 137
  - API token 649
  - computers with sensor 129
  - integrating with Bit9 Server 648
  - sensor status 137
  - sensor tamper protection 248
- Categorized Files view 194
- category. See file category
- CEF. See ArcSight integration
- certificate rules 293
- Certificates page 295
- certificates, Bit9
  - and console login 48
  - for agent-server communication 623
  - using SAN in 625
- certificates, file-signing
  - alerts for 303
  - algorithm options 245
  - and publisher approvals 242
  - approval configuration options 304
  - approving and banning 304, 306
  - approving by 236
  - certificate details fields 297
  - certificate global state 308
  - certificate path 299
  - configuring approvals by 243, 630
  - cosigner 305
  - countersignature options 245
  - detached 236, 303, 305
  - discovery and control of 293
  - effect on global file state 314
  - embedded 305
  - enabling/disabling bans by policy 313
  - events for 303
  - expired 244
  - feature overview 294
  - finding child certificates 301
  - finding events for a certificate 301
  - finding files signed by 301
  - for publisher approvals 236
  - in external views 304
  - information in file details 302
  - key length options 245
  - other rules and certificate global state 313
  - path differences 306
  - path position of 297, 306
  - policy setting for 159
  - revocation checks 245
  - table of 295
  - types 305
  - viewing details 300
  - viewing for a publisher 301
- Check Point
  - analyzing files with 734
  - enabling Bit9 integration with 698
  - enabling file analysis with 707
  - proxy settings or 708
- CIM
  - mappings for Splunk 777
- CL. See configuration list
- CLI management privileges 615
  - and command line reporting 492
- cloned computers
  - cleanup of 185, 187
  - deleting 185, 187
  - file inventory choices 185
  - managing 175
  - server backlog for 183
- command lines
  - reporting in events 492
- company
  - viewing files by 194
- Computer Details
  - Carbon Black tab 137
- Computer Details page 132
- computer security alert 496
- computers
  - adding 146
  - assigning policies 111
  - changing policies 143
  - cloned 175
  - connected (viewing) 129
  - deleting 146, 629, 630
  - details about 132
  - disconnected (viewing) 129

- duplicate registrations 485
- health check for 134
- in Local Approval (viewing) 129
- initializing 100
- installing Bit9 Agent on 113
- placing in local approval mode 260
- remote reboot of 142
- requiring upgrade, (viewing) 129
- restoring from local approval mode 261
- template computers 175
- timed Enforcement Level override for 262
- uninstalling agent on 127
- viewing AD details about 111
- viewing connection status 128
- virtual machines 175
- with/without specified files 197

Computers page 119, 129

configuration list

- current (for server) 129
- file state and 209
- for an agent computer 136

confirm navigation dialog

- enabling/disabling 71

connected computers, viewing 129

connected Enforcement Level 154, 170

connection status (agent) 134

connector. See Bit9 Connector.

console menu 53

console, Bit9. See Bit9 Console

console. See Bit9 Console

control mode 153

- enabling for a policy 151
- licenses for 640
- overview 44

cosigner certificates 305

countersignatures (for certificates) 245

countersigner certificates, see cosigner certificates

CSC temporary files 248

custom rules

- do not track example 371
- exporting and importing 359
- in visibility mode 338
- overview 336
- trusted paths 367

## D

dashboards 567

- adding portlets to 583
- baseline drift portlets in 542
- changing appearance of 576
- changing color of 578
- changing width of 578
- copying 582
- creating 579
- editing 579, 583
- home page 50
- layout of 577
- managing 579
- portlets on 570
- sharing with other users 580
- system 573
- viewing 568, 573

data analytics 759

- preparing for 760

database, Bit9

- address 613
- authorization type 613
- configuration information 612
- database limit alert 495
- events in 617
- external 619
- restoring 634
- schema version 613
- size 613
- unique files 41
- verification failed alert 495
- views via live inventory SDK 659

debug level

- for an agent computer 136

default policy 160

default starting page 71

deleted computers 146

deleted file state 218

deleted files

- searching for 605
- viewing 194

detached certificates 303, 305

detection, threat 547

device paths, in Bit9 rules 347

devices

- acknowledging 322, 323

- all devices on computers 330
- approving and banning 315
- control in Bit9 317
- device catalog 326
- managing 315, 320
- managing by model 321
- managing individual devices 325
- per-policy control 317
- policy settings 318
- rules for 316
- DFS
  - and Windows 2003/XP 116
- diagnostic files 741, 754
  - viewing 743, 754
- directory policies. See custom rules
- disabled mode (agent) 153, 167
- disconnected computers
  - and file searches 600, 604
  - and policy deletion 103
  - changing Enforcement Level 262
  - deleting 629, 630
  - during lockdown 171
  - timed deletion 629, 630
  - viewing 129
- disconnected Enforcement Level 154, 170
- display preferences 71
- DMG files
  - for installing Mac agents 116
- Download Agent Packages page 113
- downloading
  - agent installers 112
  - Bit9 data to CSV files 68
- drift reports. See baseline drift
- duplicate computer registrations 485
- dynamic code execution (memory rule) 414
- dynamic tables 58
  - downloading data from 68
  - filtering results 62
  - hiding columns 64
  - Saved Views in 66
  - showing columns 64
- E**
- email
  - address in approval request 469
  - address in SSL certificate 625
  - for alerts 494, 635
  - for approval requests 473
  - generated by block notifier link 452
  - login account user address 84
- embedded certificates 305
- emergency lockdown 172
- Enforcement Level
  - and policy settings 150
  - changing 169
  - connected 154, 170
  - defined 6, 166
  - disconnected 154, 170
  - effect on policy enforcement 167
  - file blocking for active policy settings 167
  - High (Block Unapproved) 166
  - local approval 169
  - locking down all computers 171
  - Low (Monitor Unapproved) 167
  - Medium (Prompt Unapproved) 166
  - None (Disabled) 167
  - None (Visibility) 167
  - out of date on agent 130
  - overview 44
  - setting for new policies 154
  - timed overrides of 262
- event rules 423
  - creating alerts for 498
  - disabling 426
  - enabling 426
  - ranking of 435
- events
  - agent health check 139
  - archives of 493
  - creating alerts for 498
  - creating reports of 490
  - editing reports of 491
  - events page 487
  - external logging 619
  - home page summary 483
  - log files 617
  - logging of 617
  - overview 482
  - reporting command lines in 492
  - saved views of 484, 490
  - Syslog message severity 490
  - threat detection 558

- triggering actions with 423
  - types 484
  - events integration
    - See the separate Bit9 Events Integration Guide
  - exceptions
    - for indicator sets 553
  - executables
    - advanced policy settings for 158
    - defined 39
  - Existing Files view 194
  - expired certificates
    - and certificate approvals 305
    - and publisher approvals 244
  - export directory for external analytics 765
  - exporting data 68
    - data analytics 759
  - exporting rules to another server 359
  - external analytics
    - accessing external tools from Bit9 console 770
    - creating a rule to ignore logs 767
    - data format for 761
    - enabling connection for 767
    - enabling in Bit9 Console 763
    - export directory for 765
    - exported files 761
    - installing Splunk app for Bit9 769
    - installing Splunk Universal Forwarder 769
    - viewing Bit9 data 770
  - external event logging 619
  - external notifications 718
    - event rules for 423
    - trimming 718
  - external views
    - Bit9 database 659
- F**
- file and path rules enforcement (policy setting) 159
  - file and path rules. See custom rules
  - file bans. See bans
  - File Catalog tab 217
  - file category
    - defined 207
    - drift by 526
  - file creation control 336
  - file details 205
  - File Details page 276
  - file execution control 336
  - file extensions
    - script rules and 376
  - File Group Details page 215
  - file groups
    - and initialized files 196
    - overview 202
    - viewing files in 215
  - file hash bans 227
  - File Instance Details page 210
    - initiating Find Files from 600
  - file instances
    - file name 212
    - path for 212
  - file integrity control 336
  - file inventory 36
    - excluding MS support files 198
    - of cloned computers 185
  - file name bans 43
  - file rules
    - approvals 269
    - bans 269
    - removing 271
  - file state 41, 217
    - and certificate global state 314
    - approved 217
    - banned 217
    - banned (local) 218
    - defined 7
    - deleted 218
    - flags affecting 205, 217
    - global 205
    - instance states 218
    - local 218
    - local state details 219
    - locally approved 218
    - unapproved 218
  - file state reason 205
  - file tracking
    - and alerts 494
    - disabling for a path 371
    - enable/disable by policy 155

- excluding MS support files 198
  - using baseline drift 522
  - files
    - acknowledging 209
    - analyzing in Bit9 Software Reputation 645
    - analyzing with third-party devices 687
    - approving. See approving files
    - banning. See banning files
    - baseline drift of 522
    - Bit9 database 41
    - blocked file alerts 498
    - blocking 167
    - blocking by custom rule 336
    - blocking by device rule 316
    - blocking by script rule 376
    - categories of 194
    - diagnostic 741, 754
    - executable 39
    - existing 194
    - file groups 215
    - finding 600
    - finding computers with/without specified files 197
    - first-seen name 205
    - including deleted files in a search 605
    - initializing 100
    - installing on a locked-down computer 258
    - live inventory of 36
    - local approval 252
    - locating executables on computers 602
    - malicious 194
    - marking as installer 265
    - marking as not installer 265
    - metering executions 517
    - monitoring specific executions 516
    - on deleted computers 605
    - on disconnected computers 604
    - path for first-seen 205
    - prevalence alerts 498
    - propagation alerts 498
    - reputation 282
    - show individual files 273
    - snapshots of 539
    - threat level for 207
    - tracked in Bit9 Security Platform 39
    - tracking drift 521
    - trust rating for 207
    - uploading from agents 747
    - viewing removed 194
  - Files on Computers tab 42, 218
  - filtering
    - data in portlets 595
    - table data in portlets 592
    - table results 62
  - Find Files page
    - overview 601
    - Saved Views in 606
  - finding computers
    - with/without specified files 197
  - finding files
    - case sensitivity 602
    - computers with/without specified files 197
    - from Computer Details page 139
    - from Find Files page 600
    - from Home Page 51
    - on computers in a policy 165
    - overview 600
    - special cases 604
    - using filters in a search 602
    - viewing all unapproved files in a policy 169
  - FireEye
    - access to console from Bit9 Console 730
    - analyzing files with 734
    - enabling Bit9 integration with 709
    - integration with Bit9 687
    - limiting notifications from 717
    - notifications from 718
    - threat level mappings 716
  - flags (file state) 217
  - fuzzy hashing 207
- ## G
- global state 205
  - graphs
    - displaying network information in 567
  - group information (file details) 208
  - groups
    - trusted for installation 234
  - groups (file details) 208

**H**

- hashes
  - approving 276
  - approving a list of 277
  - banning 43, 276
  - banning a list of 277
  - fuzzy hashing 207
  - identifying unknown 643
  - MD5 207
  - SHA-1 207
  - SHA-256 207
- health check
  - for agents 134, 139
- help
  - for Bit9 Security Platform 73
  - for portlets 572
- hiding table columns 64
- High (Block Unapproved) Enforcement Level 166
- High Enforcement Level
  - installing software on computers in 258
  - switching to 169
- home page 50
  - changing appearance of 576
  - changing default for new users 584
  - editing 579
  - resetting to default 584
- HP ArcSight. See ArcSight integration

**I**

- importing rules from another server 359
- indicator set details 551
- indicator sets
  - enabling and disabling 551
  - exceptions to 553
  - for threat detection 549
  - updates to 557
- information button
  - for portlets 572
  - on Active Directory Policy Mappings page 109
- initialization 6
  - and local approval 252
  - of cloned computers 185
  - of computers 100
  - status of 137

- initialized files
  - overview 196
  - viewing for one computer 216
- installed programs 202
- Installed Programs view 194
- installer (override) file flag 218
- installer file flag 218
- installers
  - and file groups 202
  - Bit9 Agent 113
  - defined 265
  - files approved as 219
  - files identified as 205
  - files marked as 209
  - in trusted directories 229
  - marking file as 265
  - recognized in trusted directories 229
  - top level 219
- installing
  - Bit9 Agent 113
  - Bit9 Server. See Installing Bit9 Server guide
- inventory (file)
  - of cloned computers 185
- IPv6
  - in server address 613

**J**

- Java
  - script rules for 377
  - updater for 248
- JSON
  - data export format 761
- justification (for user-initiated approvals)
  - alert for 496
- justifications (for user-initiated approvals)
  - alert for 496
  - customizing the notifier interface 479
  - details page 476
  - enabling in Windows 468
  - how users submit 469
  - in blocked-file notifiers 467
  - responding to 473
  - viewing in Bit9 Console 470

## K

- kernel memory access (memory rule) 414
- kernels, Linux. See separate Operating Environment Requirements guide
- key length (for certificates) 245

## L

- LEEF. See QRadar integration
- licenses, Bit9 640
  - adding 641
  - and local approval mode 258
  - Bit9 Software Reputation Service 643
  - for file uploads 748
  - managing 640
  - viewing limits and usage 640
- licenses, Bit9
  - for Bit9 Connector 689
- Linux computers
  - installing agent on 117
  - manual agent upgrades on 125
  - uninstalling agent from 128
- live inventory
  - and baseline drift 522
  - and executable files 39
  - and finding files 600
  - database views of 659
  - defined 36
  - SDK 659
- local approval 252
  - of all unapproved files on a computer 257
  - of files 252
  - of one file 255
  - removing 256
- local approval mode 258
  - alert for 495
  - and disconnected computers 262
  - and online computers 260
  - restoring computers to original policies 261
  - setting time-duration alerts 498
  - timed Enforcement Level changes 263
  - viewing computers in 129
- local file state 218
- local file state details 219
- locally approved (local state detail) 219

- locally approved auto (local state detail) 219
- locally approved state 218
- lockdown
  - Enforcement Level for 166
  - locking down all computers 171
  - restoring after 172
- lockdown. See also High Enforcement Level
- log files
  - managing 617
- logging in 48
- logging out 49
- login accounts, Bit9
  - administrator 84
  - creating new groups 90
  - defined 7
  - deleting 87
  - disabling 88
  - groups 89
  - permissions for Bit9 Connector 718
  - power user 84
  - read only 84
  - role-based access 90
  - setting preferences for 71
  - unauthorized 84
  - using AD accounts 77
- login accounts, console 76
- logo
  - specifying for notifier 460
- Low (Monitor Unapproved) Enforcement Level 167
  - file execution warnings in 169
  - switching to High Enforcement from 169

## M

- Mac computers
  - App Store updater 246
  - Bit9 tray icon on 446
  - blocked file notifiers on 444
  - installing agent on 116
  - manual agent upgrades on 124
  - native updater support for 246
  - submitting approval requests from 469
  - Symantec Endpoint Protection updater for 249



- uninstalling agent from 128
- Mac System Updates 248
- macros, in Bit9 rules 347
- malicious files
  - alerts for 495
  - how specified
- Malicious Files view 194
- Mark as installer/not installer 265
- Medium (Prompt Unapproved) Enforcement Level 166
- memory rules 407
  - editing notifier message for 409
  - exporting and importing 359
  - operating system restrictions 408
  - parameters of 411
  - viewing associated events 408
- memory rules enforcement (policy setting) 159
- meters (software execution) 516
  - creating 517
- Microsoft .NET updates 248
- Microsoft Office Click-to-Run updates 248
- Microsoft Security Essentials 692
- modes
  - overview 44
  - setting for policies 153
- monitor. See Low Enforcement Level
- MSI files
  - and trusted directories 229
  - for installing Windows agents 114

## N

- network security devices
  - notifications from 718
- new certificate alerts 303
- New Unapproved Files view 194
- not installer (override) file flag 218
- notifications
  - external 718
- notifiers for blocked files
  - conditional messages in 455
  - configuring 450
  - customizing the logo for 460
  - defined 163

- disabling 452, 463
- editing 450, 453
  - editing by policy setting 449
  - editing the source line in 460
- enabling approval requests in 467
  - for terminal servers 464
  - for XenApp 464
- history window for Mac 446
- information links in 452
  - on Mac computers 444
- timeouts for on-screen display 452
  - using tags in 454
- NT authorization
  - for database server 613

## O

- object previews
  - in table data 70
- offline computers. See disconnected computers
- online computers. See connected computers
- online help 73
- operating strategies 45
- OS X. See Mac computers

## P

- packages
  - by publisher/company 194
  - Mac .pkg files 196
  - trusted 194, 232
- Palo Alto Networks
  - access to console from Bit9 Console 730
  - enabling Bit9 integration with 692
  - file analysis with WildFire 696
  - Integration with Bit9 687
  - notifications from 718
- Parity Agent. See Bit9 Agent
- Parity Console. See Bit9 Console
- Parity Knowledge Service. See Bit9 Software Reputation Service
- Parity Server. See Bit9 Server
- Parity. See Bit9 Security Platform
- passwords
  - Bit9 Console 84
  - Bit9 Console (changing) 85

- CLI management 615
- path
  - certificate 299
  - first-seen file 205
  - trusted 367
- path position, certificate 306
- path position, for certificates 297
- path rules. See custom rules
- pending files. See unapproved files
- performance optimization
  - custom rules for 336
- policies
  - AD mapping 103
  - creating 151
  - default 160
  - defined 6, 43
  - deleting 173
  - disabling enforcement 153
  - Enforcement Level for 154
  - for uninstalling an agent 127
  - mode choices 153
  - moving computers between 143
  - related views menu 165
  - setting alerts for 498
  - template 160
  - templates for 154
  - viewing unapproved files in a policy 169
  - when assigned 111
- Policies page 152
- policy settings
  - and Enforcement Level 150
  - blocking for different Enforcement Levels 167
  - creating a template policy for 161
  - device control 323
  - editing 163
  - enable/disable file tracking 155
  - local approval of unapproved files on Enforcement Level change 253
  - notifiers for 449
  - options for 156
  - removable device 318
- policy specific states (file details) 207
- policy status 130
- portlets 570
  - adding to a dashboard 583
  - baseline drift 542
  - creating 588
  - deleting 587
  - editing 73, 587
  - filtering data in 595
  - filtering table data in 592
  - moving on dashboard 578
- potential risk files
  - alerts for 495
  - Bit9 SRS information about 207
- power users (console login) 84
- preferences, console user 71
- prevalence of files on computers 205
- printer driver updates 248
- prioritizing agent updates 140
- privileges, login account
  - administrator 84
  - and AD accounts 77
  - customizing 89
  - power user 84
  - read only 84
  - revoking 84
- process protection. See memory rules
- processes
  - in custom rules 353
  - in memory rules 415
  - in registry rules 398
  - in script rules 376
  - terminating if banned 279
- promote (treat as installer)
  - in custom rules 342
  - notifier option 443
- promoted process 353
- propagating files
  - setting alerts for 498
- proxy settings
  - Bit9 SRS 643
  - Check Point 708
- publishers
  - acknowledging 236, 240
  - and global file state 205
  - approving 236
  - approving by reputation 282
  - banning 237
  - certificates for 301
  - detached publisher state 212
  - in file details 206, 212

- policy setting for 159
  - publisher details 220
  - publisher state 206
  - viewing files by 194
- Q**
- QILabs. See QRadar integration
  - QRadar integration
    - specifying LEEF as Syslog format 623
- R**
- read only console logins 84
  - reboot
    - of agent computers 142
  - Red Hat Prelinking 249
  - refresh page 59
  - registration of Bit9 Agents 111
  - registry rules 389
    - editing notifier message for 394, 396, 399
    - enabling by policy 159
    - exporting and importing 359
    - parameters of 394
    - process menu options 399
    - write actions 396
  - registry rules enforcement (policy setting) 159
  - removable devices. See devices
  - Removed Files view 194
  - Report Process Create rule
    - and command line reporting 492
  - Report-Only (for file bans) 227
  - report-only ban flag 218
  - reputation approvals 281
  - reputation services. See Bit9 Software Reputation Service
  - reputation-based rules 281, 282
  - resizing table columns 59
  - Restore page 172
  - restoring
    - Bit9 database 634
    - computers in emergency lockdown 172
    - local-approval computers to policies 261
  - revocation checks (for certificates) 245
  - revoked certificate alerts 303
  - role-based access. See login accounts
  - rules
    - exporting and importing 359
- S**
- SAN (subject alternative name)
    - in certificate definition 625
  - Saved Views
    - creating 67
    - discarding changes to 67
    - overview 66
  - script processors 376
  - script rules 376
  - scripts
    - blocking unapproved 158
    - custom definitions of 375
    - defined 376
    - editing rules for 375
  - SecCon. See Enforcement Level
  - security domain
    - for AD integration 614
  - self-protection. See tamper protection
  - server backlog
    - for cloned computers 183
  - server, Bit9. See Bit9 Server
  - shared drives
    - file execution setting for 159
  - shortcut links 71
  - Show deleted files box
    - in Find Files results 605
  - Show Individual Files box 273
  - show/hide columns 59
  - show/hide filters 59
  - show/hide snapshots 59
  - showing table columns 64
  - SIEM integration 619
    - See also the separate Bit9 Events Integration Guide
  - silent blocks
    - in memory rules 413
  - silent blocks. See also notifiers for blocked files
  - snapshots
    - adding drift results to 531

- creating 539
  - editing 541
  - for baseline drift reports 539
  - showing panel 59
  - software approvals. See approvals
  - software bans. See banning files and bans.
  - software metering 516
  - Software Meters page 517
  - Software Reputation Service. See Bit9 Software Reputation Service
  - Software Rules page 230
  - software updates
    - automatic updater support 246
  - Splunk
    - CIM mappings for Bit9 data 777
    - enabling data collection by 768
    - enabling data export to 763
    - installing Bit9 app 769
    - installing Universal Forwarder on Bit9 Server 769
    - viewing Bit9 data in 771
  - SQL Server
    - authorization for 613
    - for external event logging 619
  - SRS. See Bit9 Software Reputation Service
  - SSL security
    - configuring 623
  - starting page, changing 71
  - Symantec Endpoint Protection (SEP) for Mac updater 249
  - synchronization
    - agent-server 136, 137
    - and template computers 177, 184
    - with Bit9 SRS 647
  - Syslog
    - enabling for Bit9 events 622
    - integrating with ArcSight 623
    - integrating with QRadar 623
    - message severity 490
  - system backups 631
  - System dashboard 573
- T**
- tags
    - for alert messages 503
    - for approval requests 468
    - for computer identification 135
    - for customizing notifiers 454
  - tamper protection
    - for agents (policy setting) 159, 162
    - for Bit9 Server 248
    - for Carbon Black sensor 248
  - template computers
    - converting to regular computer 189
    - creating 177
    - deleting 185
    - editing 179, 184
    - viewing table of 178
  - template policy 160, 161
  - templates
    - for virtual machines 175
  - terminate processes for banned images (policy setting) 159
  - terminating processes with banned images (policy setting) 279
  - TGZ files
    - for installing Linux agents 117
  - threat detection 547
    - alerts for 562
    - and Bit9 Platform upgrades 549
    - events for 558
    - indicator sets for 549
    - monitoring reports 558
    - responding to 563
    - suspicious files 562
    - updates to 557
  - threat level mapping
    - for FireEye integration 716
  - threat level, from Bit9 SRS 207
  - timeouts for notifier display 452
  - trust rating
    - for files 40, 282
    - for publishers 283
    - from Bit9 Software Reputation Service 207
  - trusted directories 228
    - archive files in 229
    - installer files in 229
    - packages recognized by Bit9 229
  - trusted groups 234
  - trusted package
    - noted in file details 209

Trusted Packages view 194, 232  
 trusted paths 367  
 trusted users 234

## U

Ubuntu updater 249  
 unapproved (local state detail) 220  
 unapproved files  
   approving on Enforcement Level change 253  
   executables (blocking by policy) 158  
   finding all on computers in a policy 169  
   local state 218  
   local state detail 220  
   locally approving on a computer 257  
   scripts (blocking by policy) 158  
   unapproved (persisted) 220  
   viewing new unapproved 194  
 unapproved persisted (local state detail) 220  
 unapproved scripts (policy setting) 158  
 unapproved state 218  
 unauthorized users 84  
 uninstalling  
   agent software 127  
 updaters  
   alert when modified 496  
   enabling 246  
 upgrade status  
   agents 125  
 upgrading Bit9 Agent 119  
   manual upgrades 122  
 uploading files from agents 747  
   automating using event rules 423  
   changing upload location 756  
 uploads  
   of diagnostic files 741, 754  
 URLs  
   for downloading agent installers 112  
   in notifier link 452  
 user passwords  
   Bit9 Console (changing) 71  
 user preferences 71  
 users, Bit9 Console. See login accounts  
 users, trusted. See trusted users

## V

version number  
   agent config list 136  
   Bit9 Server 49  
   server config list 129  
 virtual machines  
   identifying in computer details 135  
   managing 175  
 virtual platform  
   in computer details 135, 137  
 virtualization  
   session 464  
 Visibility and Control mode. See control mode  
 visibility mode 153, 167  
   and custom rules 338  
   licenses for 640  
 Visibility Only mode. See visibility mode  
 VMware  
   identifying in computer details 135, 137  
   managing clones 175

## W

warnings  
   about non-upgraded agents 119  
   file execution 169  
   license limit 641  
 Watchlist  
   Carbon Black 648  
 wildcards, in Bit9 rules 346  
 WildFire  
   analyzing files with 734  
   integrating with Bit9 696  
   multiple notifications from 724  
 Windows 2000 domain controllers  
   and Bit9 AD integration 614  
 Windows computers  
   enabling file approval requests for 468  
   installing agent on 114  
   manual agent upgrades on 122  
   submitting approval requests from 469  
   uninstalling agent from 127  
 Windows Defender updates 249  
 Windows Installer Transform files (not supported) 114  
 Windows updates 249