



Installing the Bit9 Server

Product Version: [7.2.1](#)

Document Date: [4-April-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 - 2015 The PHP Group. All rights reserved. THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED 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, 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.

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.

Installing the Bit9 Server

Document Version: 7.2.1.d

Document Revision Date: April 4, 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

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

Contents

Copyrights and Notices	2
About This Book	7
Intended Audience	8
Chapter Overview	8
Other Bit9 Documentation	8
1 Preparing for Bit9 Server Installation	11
About the Bit9 Distribution	12
Bit9 License Keys	12
Licenses for Optional Features	12
Installation Overview	13
SQL Server Account Configuration	14
SQL Server Memory Configuration	14
Installing the Platform Software	15
Network Requirements	16
Web Server Configuration	16
Supported Web Browsers	17
Browser Configuration	17
Data Export Options	17
2 Installing the Bit9 Server	19
Pre-installation Check	20
Installing the Bit9 Server Software	20
Installing a New Bit9 Server	22
Installing the Server with a Restored or Reconnected Database	36
Upgrading from a Previous Bit9 Version	50
Upgrade Installation Overview	51
Upgrade Pre-installation Requirements	52
Backup the Bit9 Server	52
Disable Software Deployment Mechanisms	53

Stop SQL Background Jobs	53
Run the Bit9 Server Upgrade Installation	53
Upgrade Installation Checks	53
Upgrade Completion	55
Review Post-Upgrade Server Configuration	55
Agent Upgrade Status.	57
Uninstalling the Bit9 Server Software	58
3 Logging In to the Bit9 Console	61
Logging In to the Bit9 Console.	62
Logging Out of the Bit9 Console	63
Changing the Administrator Password	63
Viewing User Activities in the Events Table	64
Using Help	64
Index	67

About This Book

This preface describes the contents of this publication, *Installing the Bit9 Server*.

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.*

Sections

Topic	Page
Intended Audience	8
Chapter Overview	8

Intended Audience

This manual provides information for system or network administrators who will install the Bit9 Server software and other components of the Bit9 Security Platform. Staff who install the software should be familiar with networking concepts and have experience with the Windows operating system and SQL Server management. In addition, if your site will use features that integrate the Bit9 Server and Active Directory, administrators and installers should be familiar with Active Directory concepts and use.

The Bit9 Agent can be installed on Windows, Mac/OS X, and Linux operating systems, so the installer or administrator responsible for installing and managing agents should be familiar with installing software on the supported client systems at your site.

Chapter Overview

Installing the Bit9 Server is your guide to the installation and initial configuration of the Bit9 Server. It is organized as follows:

	Chapter	Description
1	Preparing for Bit9 Server Installation	Provides an installation overview and background information helpful to know before you begin installing Bit9 Server.
2	Installing the Bit9 Server	Explains how to install (or upgrade) and start the Bit9 Server software.
3	Logging In to the Bit9 Console	Explains how to log in to the Bit9 Console.

Notes

- This guide, which focuses on Bit9 Server installation, does not include full instructions for installing third-party products, such as Windows Server, SQL Server, or products and services integrated through the Bit9 Connector. For any third-party product that you install separately for use with Bit9, see the documentation that came with the product.
- Instructions for installing the Bit9 Agent on computers to be managed by the Bit9 Server are in the “Managing Computers” chapter in the *Using the Bit9 Security Platform* guide. This is available as both online help from the Bit9 Console and as a PDF file.

Other Bit9 Documentation

You will need some or all of the following Bit9 documentation to accomplish tasks not covered in *Installing the Bit9 Server*. These documents are available through the Bit9 Technical Support website. Some of these documents are updated with every newly released build while others are updated only for minor or major version changes.

- ***Operating Environment Requirements*** – Describes the hardware and software platform requirements for the Bit9 Server, the SQL Server database that stores Bit9 data, and the Bit9 Agent.
- ***Supported Agent Operating Systems*** – Describes the supported operating systems for the current version of the Bit9 Agent.
- ***Using the Bit9 Security Platform*** – Provides complete information about configuring and operating the Bit9 Server as well as instructions for deploying and managing Bit9 Agents.
- ***Bit9 Security Platform Release Notes*** – Provides version- and build-specific information about new features, corrective content, and known issues with the release.
- ***Bit9 Events Integration Guide*** – Provides a detailed inventory of events recorded by Bit9 and includes instructions for integrating Bit9 event data with third-party SIEM systems via Syslog.
- ***Bit9 API Documentation*** – Describes the Bit9 API, which offers the ability to perform certain Bit9 Security Platform actions without using the Bit9 Console user interface. Instructions for enabling this API are in the *Using the Bit9 Security Platform* guide. Full details for the API are at: <https://github.com/carbonblack/bit9platform>

Chapter 1

Preparing for Bit9 Server Installation

This chapter describes the contents of the Bit9 Security Platform and provides an installation overview, preparation requirements, and general information about third-party applications integrated or compatible with Bit9.

This document also includes instructions for upgrading Bit9 from a previous version. However, you may receive additional upgrade documentation from your Bit9 Support representative, and, if so, you should have it available for the upgrade process.

The separate *Operating Environment Requirements* document provides guidelines for hardware and software required for the Bit9 Security Platform. Your environment must meet these requirements before you begin the procedures described in this document.

Note

Bit9 Platform v7.2.1 includes a new System Health page that uses health indicators to report on your system. A prime purpose of these indicators is to monitor compliance with the Operating Environment Requirements and report any non-compliance so that you can remedy it. See “Monitoring System Health” in *Using the Bit9 Platform* for more information.

Sections

Topic	Page
About the Bit9 Distribution	12
Bit9 License Keys	12
Installation Overview	13
Network Requirements	16
Web Server Configuration	16
Supported Web Browsers	17

About the Bit9 Distribution

Bit9 supplies the Bit9 Server installation program as a download. New sites will also receive a Bit9 license key to be used during installation.

Table 1: Bit9 Distribution Contents

Contents	Description
Bit9 Software	The Bit9 Server installation files. Bit9 Agent installers are created through the Bit9 Console after the server is installed.
Documentation	The Bit9 Console includes online Help describing Bit9 Security Platform features and procedures, including how to install the Bit9 Agent on endpoints. You can view the Help contents page by choosing Help in the console menu. <i>Context-sensitive Help</i> can be launched by clicking the Help (?) button on any console page. PDF versions of this and other user documentation can be downloaded by logging to the Bit9 Customer Support Portal .

Bit9 License Keys

The Bit9 Server can be licensed at two primary feature levels:

- **Bit9 Visibility:** This level provides all of the Bit9 Security Platform's file and event tracking and reporting capabilities, but does not include support for control features such as file bans and device blocking.
- **Bit9 Suite:** This provides both Visibility and Control capabilities.

Licenses are based on the number of agents running at each level. You can mix licenses on the same server, having, for example, 20 Visibility licenses and 50 Suite licenses. In addition, you can purchase upgrades to bring Visibility licenses up to full Bit9 Suite level.

Important

During a new server installation, you will be prompted for a license key. Have this key available before you begin installation. A new installation completed without a license key is a full-featured, 30-day evaluation version (without special options). You can add or upgrade a license key after installation, on the System Configuration page of the Bit9 Console.

Upgrade installations and reconnections to existing Bit9 databases do not require a new license key, but if one is provided by Bit9, apply it during the installation process. For instructions on adding licenses after installation, see the "Bit9 Configuration" chapter in the *Using the Bit9 Security Platform* guide or online Help.

Licenses for Optional Features

In addition to determining the number of licensed agents and their mode, the license key can add optional features to your Bit9 installation, including the Bit9 Connector for Network Security Devices and the File Upload feature. To use these features, be sure to obtain the correct license from Bit9.

Installation Overview

The Bit9 Security Platform includes server and agent components. Server software installs on standard Windows-Server-based computers, and can be run on a virtual machine. The server installation procedure handles all operating system configuration except for IIS, for which you must follow the configuration on page 16.

Agent software installs on server, desktop, and laptop computers, and on POS (point-of-sale) systems; it may be installed on Windows and Mac systems that meet the *Operating Environment Requirements*. The agent provides initial security rules to endpoint computers and enables connected systems to interact with the Bit9 Server for ongoing management. .

Note

Downloadable Bit9 Agent installers are created dynamically by the server according to protection levels you specify for computers associated with a policy. Separate media is not provided or required for agent installation. Instructions for installing the Bit9 Agent appear both in the “Managing Computers” chapter of the *Using the Bit9 Security Platform* guide and online console help.

A Bit9 Server installation follows these high-level steps:

Step 1: Determine your appropriate hardware and database configuration.

The Bit9 Server and its database may be set up on a single system. Depending upon your own preferences and the number of clients you will manage with Bit9, you may require a dedicated system for a database server and/or for a Syslog server. You also may install the Bit9 Server and agents in a virtualized environment. See the *Operating Environment Requirements* document to determine the right choices for your environment.

Step 2: Procure the required hardware for the Bit9 Server.

Step 3: Install Windows Server, IIS, and .NET on the Bit9 Server hardware.

Use a clean Windows Server installation with all the latest patches from Microsoft. Then install the Internet Information Services (IIS) version supplied with your Windows Server, using the configuration described in “Web Server Configuration” on page 16. Also, make sure that both Microsoft .NET 3.5 and 4.5 frameworks are installed with the default settings and the latest patches.

Step 4: Confirm that you have Windows Installer 4.5 on the Bit9 Server system.

The Bit9 Server installer requires that you have Windows Installer 4.5 (or greater). You can check the Windows Installer version by typing `msiexec /?` at a command prompt.

If necessary, you can download Windows Installer 4.5 from the following location:

<http://www.microsoft.com/download/en/details.aspx?id=8483>

Step 5 - option 1: Install your own licensed copy of SQL Server on the same system as the Bit9 Server *before* you install the Bit9 Server.

Follow the SQL Server configuration instructions in the *Operating Environment Requirements* document; in particular, note whether the number of endpoints you plan to manage requires the use of option 2.

- or -

Step 5 - option 2: To use a remote database server, procure the hardware, operating system, and your own licensed copy of SQL Server, then prepare the system.

Connect the SQL Server hardware to the Bit9 Server hardware by a minimum latency, gigabit backbone.

Step 6: Install and configure the Bit9 Server software.

Install the Bit9 Server software on the dedicated computer.

SQL Server Account Configuration

The user account that will access a remote Parity database must have the following permissions:

Permission	Required	Reason
Create Any Database	Yes, during installation.	This permission is required during product installation, and can be revoked after installer finishes.
View Server State	Yes	Allows collection of Bit9 Security Platform performance statistics
View Any Definition	Yes	Allows collection of Bit9 Security Platform performance statistics
Alter Trace	Yes	Allows collection of on-demand SQL trace for performance diagnostics
Alter Server State	No (Recommended)	Allows server to reset performance counters on daily basis, and provides better performance diagnostics

Note that many of these permissions allow server metrics to be collected by Bit9 for monitoring of the internal health of the server and to provide diagnostics in case of SQL database issues. This information is very important in helping Bit9 support your server installation, and also provides server performance data that may contribute to future product improvements.

In addition to the permissions shown in the table, the Bit9 service account must remain db_owner after the server is installed.

SQL Server Memory Configuration

If you are using a single-tier configuration, that is, Bit9 Server and SQL Server installed on the same system, you should configure the SQL Server to use shared memory for the

connection to gain the maximum performance benefit of the single-tier architecture. Use of TCP for the introduces unnecessary latency into the system.

Follow these configuration guidelines to make the SQL Server to use shared memory for its connection to the Bit9 Server when they are on the same machine:

- Do not use a FQDN to specify the SQL Server name -- it causes the server to use TCP for the connection. To make the SQL Server connection use shared memory instead, use a local server name.
- Make sure that Shared Memory protocols are enabled for both network and client configuration in the SQL Configuration Manager.

Installing the Platform Software

Follow these guidelines for installing or upgrading platform software for the Bit9 Server:

1. Ensure that the server is a dedicated, trusted computer that uses the NTFS file system, not FAT or FAT32.
2. If you are repurposing another computer to use as the Bit9 Server, reformat the disk. During reformatting, select NTFS (the default file system).

Important

- Commercial servers commonly bundle vendor-specific server-management utilities with Windows Server. If you install the Bit9 Server on a server platform that is bundled with such utilities, there might be unexpected interactions between the utilities and Bit9.
- If your company has any server-hardening procedures that you intend to use on this server, contact Bit9 Support to confirm that the Bit9 Server will run in the environment you create.
- Apply server-hardening procedures *before* installing the Bit9 Server.

3. If the operating system is not preinstalled, follow the standard Microsoft instructions for installing it. Be sure you are using the US English version. Bit9 recommends that you select the default installation options.
4. If you have a network domain and you want to use the Bit9 Server's Active Directory integration, add the server to the domain.
5. Install Internet Information Services (IIS) — you may need the Windows Server media. See [“Web Server Configuration”](#) on page 16 for the required IIS configuration.

Note

Once IIS is installed, you cannot change the server name and still have IIS function correctly. If you need to change the server name for any reason, contact Bit9 Support.

6. If you currently have an earlier version of Windows than those listed in the Bit9 operating system requirements, upgrade to the required version and service pack.

7. Install Microsoft .NET 4.5 Framework on the Bit9 Server. If necessary, go to <http://www.microsoft.com/downloads> and choose the latest version for download.
8. Download and install any current patches for each element of the platform software.

Network Requirements

See the *Operating Environment Requirements* document for full network details. In addition to the requirements described there:

- If you intend to use the Active Directory integration features of the Bit9 Server, the server must be a member of a domain. See the *Using the Bit9 Security Platform* guide for more information on Active Directory integration features.
- Bit9 recommends that your Bit9 Server have access to a remote network share for backup purposes, or that you make other reliable backup arrangements.

Web Server Configuration

The Bit9 Server works with IIS 7.5 on Windows Server 2008 R2 or IIS 8.0 on Windows Server 2012 R2. Do a clean IIS installation before you install the Bit9 Server. In normal use with Bit9, the web server starts at boot time. The Bit9 Server does not support substitution or co-installation of any other web servers.

Once IIS is installed, you cannot change the server name and still have IIS function correctly. If you need to change the server name for any reason, contact Bit9 Support.

In the **IIS Roles Manager**, verify the following configuration:

- Common HTTP Features: All
- Application development:
 - ASP.NET (*versions 3.5 and 4.5*)
 - .NET Extensibility (*versions 3.5 and 4.5*)
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
- Health & Diagnostics:
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing
- Security:
 - Basic Authentication
 - Windows Authentication
 - URL Authorization
 - Request Filtering
 - IP and Domain Restrictions
- Performance: None

- Management Tools:
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
- FTP Publishing Service: None

Notes

- Once the Bit9 Server is installed, you may remove the Basic Authentication and Directory Browsing roles if you choose.
- For Windows Server 2012, private memory for IIS should be increased to 800 MB.

Supported Web Browsers

You access Bit9 features through a Web-based user interface called the Bit9 Console. Although other browsers with HTML frame support should work, these Bit9-certified browsers are recommended:

- Microsoft Internet Explorer Version 9.0 or higher
- Mozilla Firefox latest version
- Chrome latest version
- Safari 5.1.2 or higher (on OS X only)

Browser Configuration

All browsers must be enabled for JavaScript to access to the console and online Help.

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

Data Export Options

Bit9 provides data export options including downloadable reports in CSV format, read-only views into certain elements of the database, and Syslog messaging that exposes relevant event data and statistics for programmatic analysis. For any database configuration, events will be stored in the primary Bit9 Server database. If you want to log Bit9 events to an external SQL Server, see “System Configuration” in the *Using the Bit9 Security Platform* guide. For more information on the external views into the database, see “Live Inventory SDK: Database Views” in the *Using the Bit9 Security Platform* guide.

Beginning with this release, Bit9 also supports export of events and other data to third-party analytics platforms. See “Exporting Bit9 Data for External Analysis” in the *Using the Bit9 Security Platform* guide for more information.

Chapter 2

Installing the Bit9 Server

This chapter explains how to install or upgrade the Bit9 Server. When you have successfully completed the server installation procedures, see “Managing Computers” in the *Using the Bit9 Security Platform* guide (or online help from the Bit9 Console) for agent installation and upgrade instructions.

Sections

Topic	Page
Pre-installation Check	20
Installing the Bit9 Server Software	20
Installing a New Bit9 Server	22
Installing the Server with a Restored or Reconnected Database	36
Upgrading from a Previous Bit9 Version	50
Uninstalling the Bit9 Server Software	58

Pre-installation Check

Before installing the Bit9 Server, ensure that:

- the server on which you will install it meets the requirements in the *Operating Environment Requirements* for Bit9 Security Platform v7.2.1.
- IIS is installed and configured as described in “[Web Server Configuration](#)” on page 16
- SQL Server is installed according to the requirements in the *Operating Environment Requirements* for Bit9 Security Platform 7.2.1.

Important

SQL Server is required for Bit9 Server operation and must be installed *before* you install the Bit9 Server. See the separate *Operating Environment Requirements* document for information about supported versions and configuration of SQL Server. Have the SQL Server location, instance (if any), and login information available during Bit9 Server installation.

During Bit9 installation, you will have a choice to use Windows authentication or SQL authentication to configure access to the SQL Server by the Bit9 Server. Bit9 strongly encourages using a specific Windows Domain account for installing and logging in to the Bit9 Server, and using Windows authentication for database access. For either authentication method, the account you use to access the database must be added to SQL Server with “sysadmin” checked in the Server Roles.

If dedicated SQL Server hardware is used, the Bit9 Server installer will also install the required SQL Server drivers locally on the Bit9 Server machine. The drivers installed are from SQL Server 2008 R2 and should be able to communicate with the any of the supported SQL Server versions listed in the *Operating Environment Requirements*.

Installing the Bit9 Server Software

You install the Bit9 Server using standard installation dialogs. During installation, you specify system configuration information about the server and optionally provide your own web-server certificate. You must log in as a Windows administrator to install the Bit9 Server.

The system on which you install the server must have an IP address that is visible to all computers running the Bit9 Agent, with a fully qualified DNS domain name or alias. In addition, to use Bit9’s Active Directory integration features without special configuration, the Bit9 Server must be installed in the same AD forest as:

- users you plan to allow Bit9 Console access via their AD login
- computers and users whose AD information you plan to use for automatic security policy assignment

Important

If you need to have the Bit9 Server in a different AD forest than computers and users you want to use in Bit9 integrations, contact Bit9 Technical Support for special instructions.

If you are installing a completely new Bit9 Server, follow the steps in [“Installing a New Bit9 Server”](#) on page 22.

If you are installing new Bit9 Server software with a backup Bit9 database, skip to [“Installing the Server with a Restored or Reconnected Database”](#) on page 36.

If you are upgrading from a previous version of the Bit9 Server, skip to [“Upgrading from a Previous Bit9 Version”](#) on page 50. You also might receive a supplemental document with newer instructions for an upgrade from your Bit9 Technical Support representative.

Important

Several Bit9 Server administrative features are disabled by a reinstallation or upgrade of the server. When an upgrade installation is complete, log in to the Bit9 Server and re-enable the ones you use:

- System backup is disabled. To re-enable, go to the Advanced Options tab on the System Configuration page.
- Automatic upgrades of agents are disabled. To re-enable, go to the Advanced Options tab of the System Configuration page. This should be done only after determining and configuring an upgrade plan that avoids excess load on the server and network.
- See [“Review Post-Upgrade Server Configuration”](#) on page 55 for more details about re-enabling features after an upgrade.

Installing a New Bit9 Server

These instructions are for a completely new installation of Bit9, with a new database (no restorations of or reconnections to an existing Bit9 database).

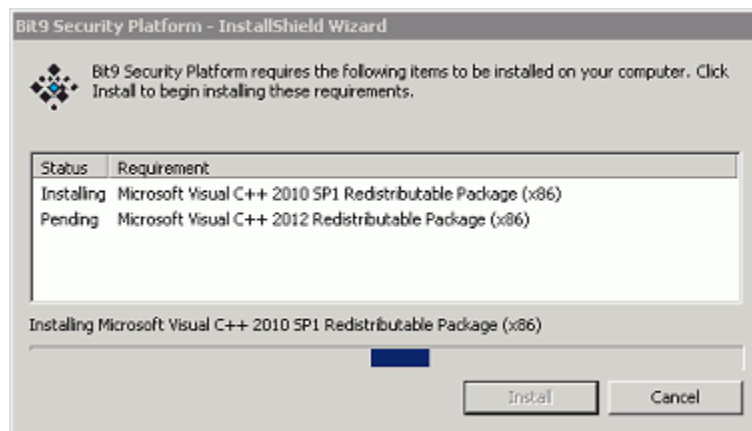
To install a new Bit9 Server:

1. Log in using an account with local Windows administrator credentials. If you plan to use Windows Authentication to login to a remote Bit9 database, install the Bit9 Server using an account that has been added to SQL Server with “sysadmin” checked in the Server Roles. Bit9 strongly encourages using a specific Domain account for installing and logging in to the Bit9 Server, and for database access, to simplify control of both database and Active Directory permissions.

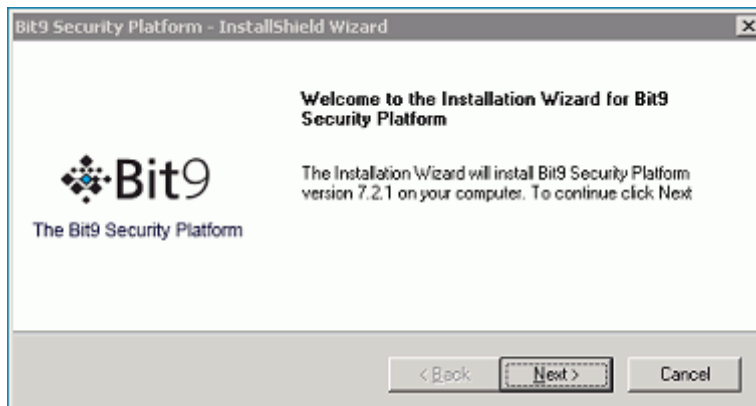
Important

Do not change the privileges of the account used to install the Bit9 Server after installation. This account must continue to have local administrator privileges for the Bit9 Server to function properly, and will also be used for server upgrades.

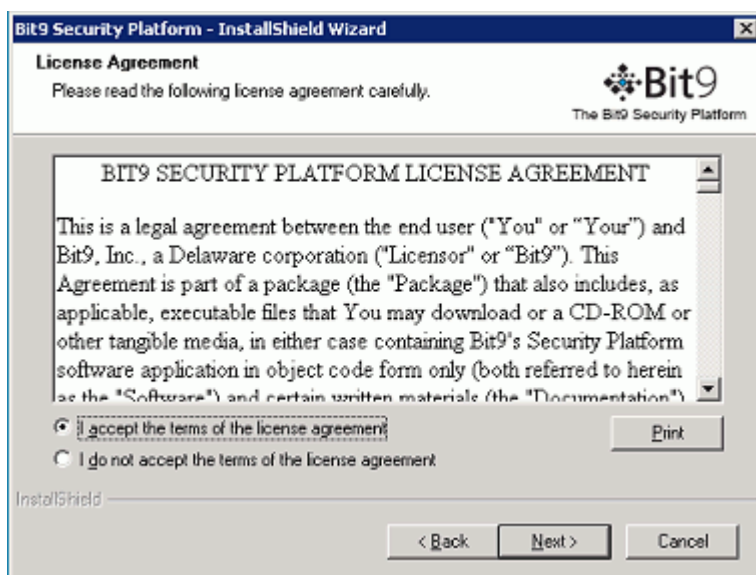
2. Make the Bit9 Server installation file available to the installation computer (either by download or inserting media in an accessible location).
3. Run the installer in either of the following ways:
 - a. To install on a local server, double-click the `ParityServerSetup.exe` file to start the installation program. Continue to the next step.
 - b. To install from a remote desktop, copy the `ParityServerSetup.exe` file to the installation computer and execute the file.
4. If the installer detects that required Microsoft redistributable packages are not present, a dialog box listing those packages appears. Click Install on the dialog to install the packages and continue with the Bit9 Platform.



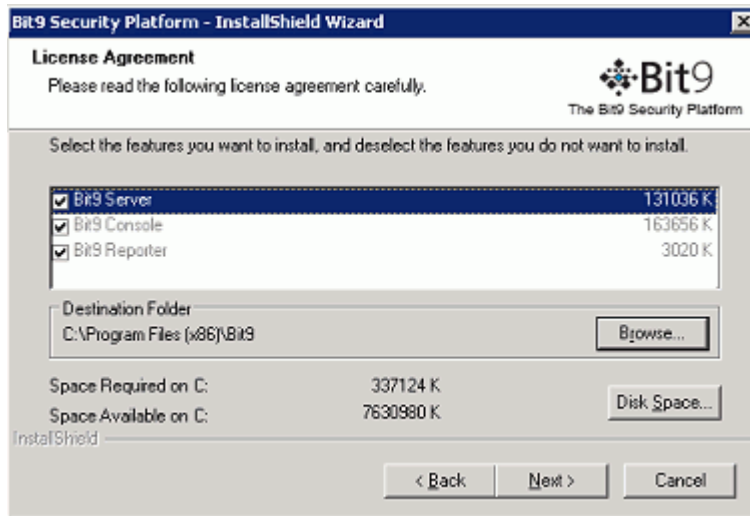
If no missing packages were detected, or when the installation is completed, the Bit9 Security Platform Welcome dialog appears.



5. From the Welcome page, click **Next**. The License Agreement screen appears.



6. Review the Bit9 Security Platform software license agreement. You must agree to the license terms to install the Bit9 Server. When you click **I accept** and continue, you agree to all terms of use. To continue, click the **Next** button. The Select Features dialog appears.



7. The Select Features screen provides information about the features being installed by Bit9, the installation folder, and the space required and available for installation:
 - a. Although they have checkboxes, Bit9 Console, Bit9 Server, and Bit9 Reporter are always installed — they cannot be deselected. Bit9 Console is the web interface to the Bit9 Server. Bit9 Reporter is the service that connects the Bit9 Server to Bit9 Software Reputation Service (SRS), which provides access to a database of file information. Reporter, which runs as a Windows service, also provides other essential reporting capabilities, including collection of support information, for the Bit9 Server.
 - b. Either keep the default installation folder (which differs from 32-bit to 64-bit systems) or click **Browse** and navigate to the folder in which you want to install the Bit9 Server. If you don't choose the default, use a path that has only valid ASCII characters, not Unicode. When you have chosen the folder, click **Next**.

Note

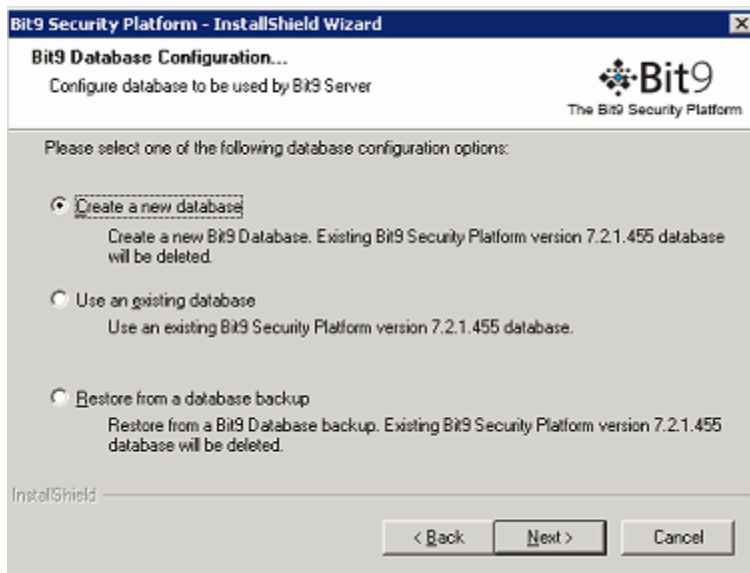
At this point in the installation, the installer program checks to be certain that it can write to the folders and registry locations needed. If any issues are found, they (and their paths) are listed in a dialog, and you must resolve them before continuing the Bit9 installation.

8. The Database Server screen appears next. It includes two configuration choices:

- a. In the Database Server field, enter the name of the SQL server, and (if any), its instance name, you are using for Bit9 data. If the SQL Server and Bit9 Server are on the same system, use a local name (not an FQDN) to allow use of shared memory for the connection between the two. See [“SQL Server Memory Configuration”](#) on page 14 for more details.
- b. With the Connect Using radio buttons, choose Windows Authentication (i.e., with the user doing the Bit9 installation) or SQL Server Authentication. If you choose SQL Server Authentication, provide the Login ID and Password. Your choice here determines how access to the SQL Server by Bit9 will be authenticated, both during and after Bit9 installation.
- c. When you have entered all database information, click **Next**.

Note: For either authentication method, the user must have been given the “sysadmin” Server Role in SQL Server.

9. The Bit9 Database Configuration Options screen appears next.

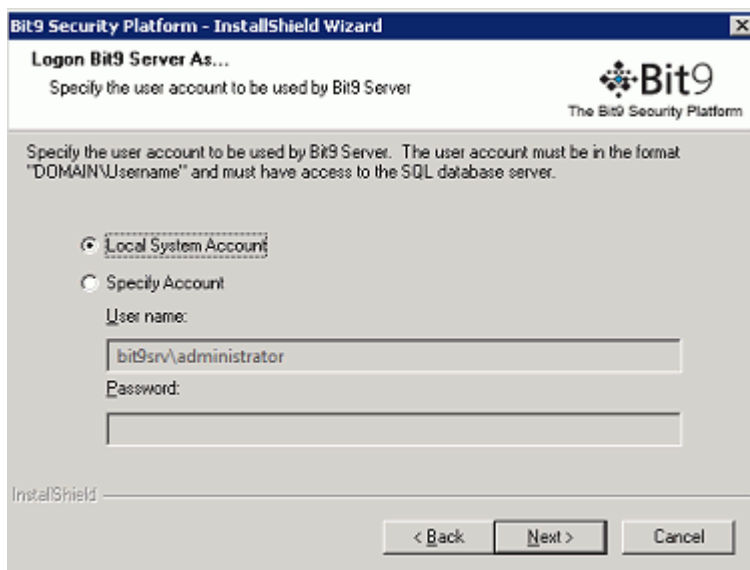


On the Bit9 Database Configuration Options dialog, choose **Create a new database** if you are installing the Bit9 Server for the first time and then click **Next**.

Note

The other database configuration options, *Use an existing database* and *Restore from a database backup*, are described in [“Installing the Server with a Restored or Reconnected Database”](#) on page 36.

10. On the Logon Information screen, choose the logon account to be used by the Bit9 Server. This will also be the account used to install future patches and upgrades. You can choose one of two modes of logging in:



- a. The Local System Account radio button instructs the installer to configure Bit9 to use the built-in Windows System account.
- b. The Specify Account radio button activates the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username and have full access to the SQL database server. The default for this choice is the currently logged in user.

Notes

- Bit9 strongly encourages using the Specific Account option to simplify control of database and Active Directory permissions. In general, the installer should be run by this same Domain account.
- For local SQL Server Express databases, the currently logged in user *must* be the same as the user specified in the Logon Information installation dialog, and the user must have the “sysadmin” Server Role. If you enter a different user, an error message appears and you must re-enter the current user.
- For remote databases, to use a Domain account to access the SQL database, you must run the installer as that account and choose the Specific Account option for that account. This user account must have the “sysadmin” Server Role in SQL Server. If you provide an invalid login account, Bit9 Server installation will fail later in the process, and you will need to reinstall.

- c. When you have provided logon information, click **Next**.

11. The Server Configuration Options screen appears next.

From the Server Configuration Options screen, review the configuration settings. In the Server Address field, the preferred address for the Bit9 Server is a fully qualified DNS name or alias that is resolvable by all computers running Bit9 Agent. Although not recommended, if the server is assigned a static IP address that will not change at reboot time, you can keep the default IP address selected for the Bit9 Server. The

installation program automatically supplies the correct information for the installation computer. The Console Port, which is used for communications between the Bit9 Server and Bit9 Console, is 41001. The Agent Port, which is used for SSL communication with Bit9 Agents, is 41002.

Notes

- Bit9 strongly recommends the use of a fully qualified DNS name or alias for Server Address whenever possible. Use of a CNAME (alias) may provide more flexibility and reliability.
- If you use multiple NICs, make sure the FQDN you use in the Server Configuration screen refers to the address of the card(s) you want the Bit9 Agents to connect to.
- An SSL certificate is automatically generated to protect communications between the Bit9 Server and its agents. If the Common name of the server does not match the server name configured here, server and agents will be unable to communicate correctly.
After installation is complete, you can replace this certificate with an existing certificate on the **Administration > System Configuration > Security** page in the Bit9 Console.

When you have reviewed the server configuration and made any necessary changes, click **Next**.

12. If you chose **Specify Account** in the (*Bit9 Server*) Logon Information screen (step 10), another Logon Information screen appears next, for *Bit9 Console under IIS*.

This screen allows you to specify different user credentials to start the IIS process for Bit9 Console, the web-based user interface for the Bit9 Server.

- a. Choose **Local System Account** to configure the Bit9 Server to use the built-in Windows system account to start the IIS process for Bit9 Console.
- b. Choose **Specify Account** to activate the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username.

Note

If you use a logon other than the current user, a warning dialog will be shown: “The Bit9 Server installer is unable to validate whether the specified account is able to access the SQL database server. Are you sure you want to continue?” If you are certain the account you provided is valid, choose **Yes**.

- c. Click **Next**.

13. The Certificate Options screen appears next. Choose the digital certificate that will appear to Bit9 Console users. You either create a certificate using a template provided by Bit9 or substitute your company's certificate.



- a. If you do not have your own certificate, choose **Create Certificate**. This allows you to create a Bit9 self-signed certificate. You can either leave Bit9's default information or supply certificate information that identifies your own organization instead. Self-signed certificates will generate warning boxes when you log in to the Bit9 Console using Internet Explorer or Firefox, although Firefox will allow you to permanently accept the certificate to eliminate future warnings. To create a certificate, choose **Create Certificate**, click the **Next** button, and skip to Step 14.
- b. To substitute your own certificate, choose **Use Pre-existing Certificate**, click the **Next** button, and skip to Step 15.

Notes

- The Bit9 self-signed certificate cannot be universally trusted because it is not created through a trusted provider such as Verisign or Thawte. This is why it generates a warning on login. While this doesn't interfere with Bit9 operation, you may want to acquire your own, trusted certificate to avoid the warning.
- It is possible that Firefox browsers will not allow use of self-signed certificates that specify the hostname as an IPv6 address. This has been a known Firefox issue: see https://bugzilla.mozilla.org/show_bug.cgi?id=633001

IPv6 itself is fully supported for the Bit9 Server, and if a FQDN representing an IPv6 address is used in the certificate, Firefox should accept the certificate.
- A self-signed certificate with a validity period greater than 20 years will not be usable. If necessary, create and use a new certificate with a shorter validity.

14. If you chose Create Certificate, the Create X.509 Certificate screen appears.

Bit9 Security Platform - InstallShield Wizard

Create X.509 Certificate for Bit9 Console (IIS)

The following information is needed to create an X.509 certificate for Bit9 Console (IIS).

Please enter the information you would like to have displayed on the X.509 certificate.

Country Code: Email Address:

State: Enter Password:

City: Confirm Password:

Company:

Department:

Common Name:

Subject Alternative Name:

InstallShield

< Back Next > Cancel

- a. By default, all certificate details correspond to Bit9 name and address data. Please replace them with details of your company. The default password is 'password'. Bit9 recommends that you change it, and keep a record of your new password so it can be retrieved for later use. The Common Name field defaults to the IP Address or DNS Name of the Bit9 Server; it cannot be changed. If the Bit9 Server is reachable by multiple DNS names, you can use the Subject Alternate Name field to specify the alternate names.
When the certificate is validated against a computer, it is validated against a Common Name or one of the Subject Alternative Name entries (if they exist). If both are present, names in the Subject Alternative Name field have priority.
 - b. When the information you want is in all fields, click **Next** to create the certificate and skip to the License Key screen (step 16).
15. If you chose Use Pre-existing Certificate, the Use Pre-existing X.509 Certificate screen appears. Enter the required information:

Bit9 Security Platform - InstallShield Wizard

Use Pre-Existing X.509 Certificate for Bit9 Console (IIS)

Select the pre-existing X.509 certificate file that will be used.

Please select the certificate for accessing Bit9 Console (IIS). Certificate is imported by specifying a certificate file (.pfx) and a password. Certificate Common Name or one of the SAN entries must correspond to the Server name.

Enter Certificate File: Browse

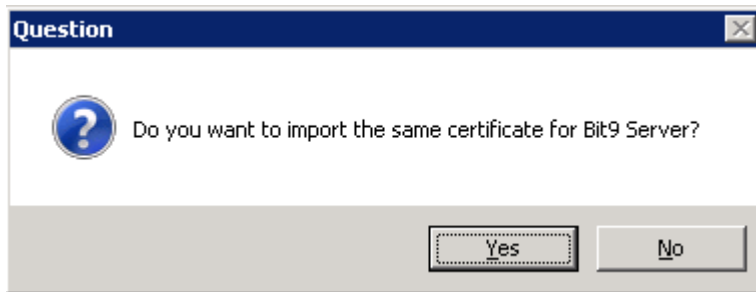
Enter Password:

Confirm Password:

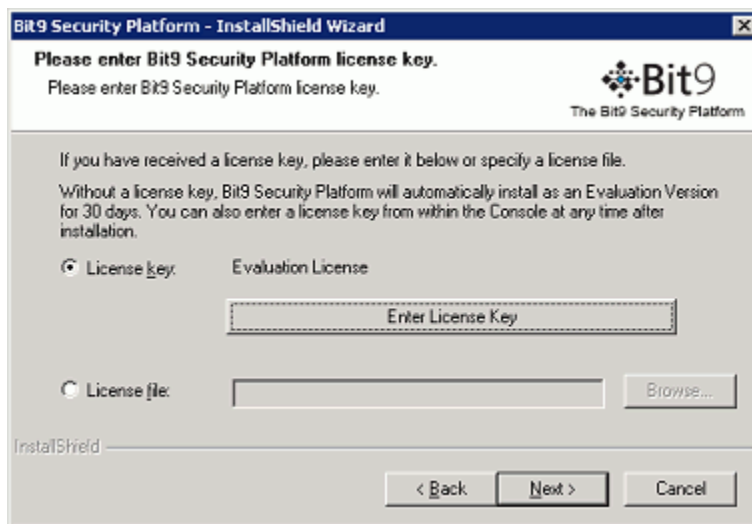
InstallShield

< Back Next > Cancel

- a. Click the **Browse** button next to the *Enter Certificate File* field, navigate to the PFX (PKCS.12) certificate file you want to use, and click **Open** when you have located the file. The filename appears in the certificate file box.
- b. Enter the password for the certificate, and re-enter it in the confirmation field.
- c. When you have entered the certificate file and the passwords, click **Next** to validate the certificate file with the password.



- d. A dialog box appears allowing you to use the same certificate for Agent-Server communications. Choose **Yes** to use the same certificate or **No** if you want Bit9 to generate a different, self-signed certificate for Agent-Server communications (you can modify this certificate or choose a new one through the Bit9 Console later). After you make your choice, the License Key screen appears.
16. On the License Key screen, you enter the license key provided by Bit9. This key determines how many agents you can run at each of the two fundamental feature levels -- Visibility-Only or Visibility-and-Control -- and may also include permission for optional features.



You have two options for entering the key:

- a. Click the *Bit9 license key* radio button if you want to cut and paste the license key (for example, from an email message or other communication).
- or-**
- Click the *Bit9 license file* radio button if you want to provide the name and path to a license file containing the key. License key files have the file extension **.lic**.

When you click this radio button, the Browse button is activated so that you can locate and select the license file using the standard Windows Choose File dialog.

Note

You do not have to enter a license key. When no key is provided, the Bit9 Server is installed with a 30-day evaluation license. After installation, you can update the license at any time from the System Configuration page of the Bit9 Console.

- b. When you have provided either the license key text or a license file, or have chosen not to enter a key, click **Next**. The Bit9 Agent Management screen appears.

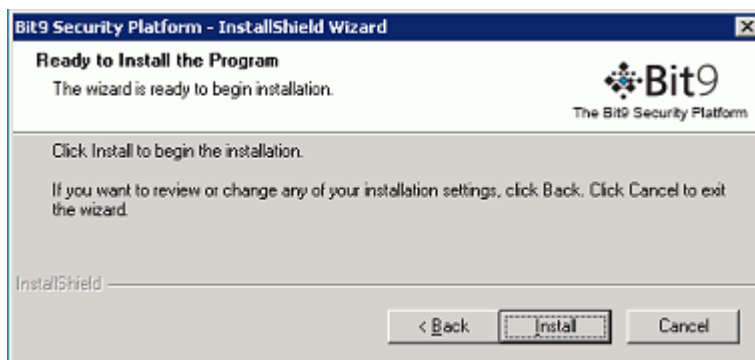
The screenshot shows the 'Bit9 Security Platform - InstallShield Wizard' window. The title bar is blue with the text 'Bit9 Security Platform - InstallShield Wizard'. The main window has a white background. At the top, there is a header section with the Bit9 logo and the text 'The Bit9 Security Platform'. Below the header, the title 'Bit9 Agent Management' is displayed. The main text area contains the instruction: 'Specify global access method(s) for Bit9 Security Platform management commands.' Below this, there is a paragraph explaining that global access can be provided by specifying a user or group, a password, or both, and that the user should choose an access option on the General tab of Administration > System Configuration page. There are two main sections for configuration: 'Specify global password for managing agents' and 'Specify user or group allowed to manage agents'. The first section has two checkboxes, both of which are unchecked. The second section has three radio buttons for 'Pre-defined group', 'User or group', and 'User or group', all of which are unchecked. Below these are three rows of input fields for 'Windows', 'Mac', and 'Linux', each with a 'User' or 'Group' radio button and a text box. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a dashed border.

17. On the Bit9 Agent Management screen, you can enable global access to agent management commands used for diagnostics, recovery, and other special situations. Although you can configure this after installing the Bit9 Server, it is highly recommended that you configure this feature before installing agents since your choice (or lack of one) is built into the agents when you install them. It is especially important to set up a global access method if you will have agents that are offline frequently or at all times. The choices are:
- Specify a global password for managing agents: Check this box, then enter and confirm a password, if you want to enable access to agent management commands on all agents via a single password.
 - Specify a user or group allowed to manage agents for each platform (Windows and Mac are supported at this time): Check this box if you want to enable access to agent management commands by choosing a pre-defined group from a menu (for Windows) or by entering a user or group name used at your site. Provide a user or group for each agent platform you have in your Bit9 environment.

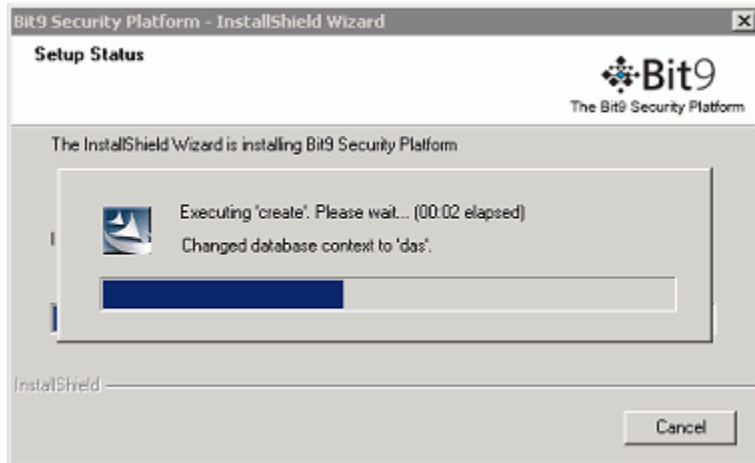
Notes

- If you define both a user/group and a password, *either* access method is sufficient on its own.
- If you plan to manage clients from computers running Vista or Windows 7, use of pre-defined Windows groups for access privileges is not recommended because Windows UAC may not provide the expected membership in a group.
- See “Configuring Agent Management Privileges” in the *Using the Bit9 Security Platform* guide for more information about configuring agent management access.

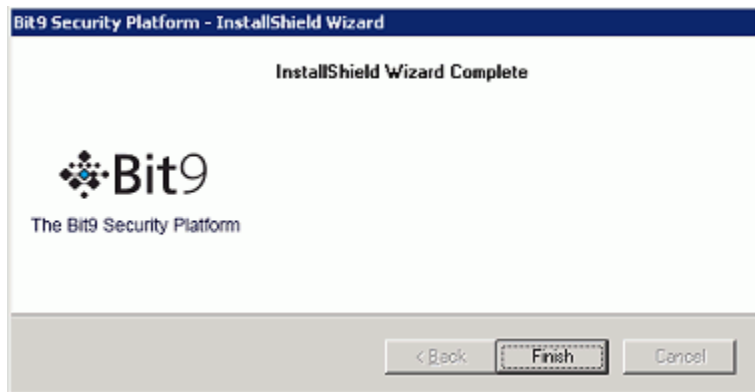
- Click **Next**. The Ready to Install screen appears.
18. If you are satisfied with your installation choices, click the **Install** button on the Ready to Install screen:



19. Bit9 Server installation begins. There is a status box overlaying the main dialog to show the progress of SQL script execution. The main dialog also has a status indicator for the overall installation.



20. When the InstallShield Wizard Complete screen appears, the installation is complete.
- In some cases, you will need to restart the server computer after installation is completed, and the dialog will include an option to restart now. Choose to restart now unless you need to complete some other activity on this computer.
 - Click the **Finish** button. Bit9 Server, which runs as a service, begins to operate after you click this button. Installation logs are placed in the Bit9 installation folder (for example, *C:\Program Files (x86)\Bit9*).



Installing the Server with a Restored or Reconnected Database

The Bit9 Server installation program provides the option of reconnecting to an existing database. In addition, you can restore a database from backup, if necessary, and then reconnect to that.

- If your database server and the Bit9 Server are on the same machine, you can *reconnect* to an existing database or *restore* the database from backup using the procedure below. The Bit9 Server installation program will prompt you for all necessary information.
- If you have a remote Bit9 database and that database is operational, you can *reconnect* to it using the procedure below. The Bit9 Server installation program will prompt you for all necessary information. *Restore* is not an option for remote databases.
- If you need to *restore* a Bit9 database on a remote system, contact Bit9 Support for instructions.

Important

- When you reinstall the Bit9 Server or upgrade to a new version, system backup and automatic agent upgrades are disabled. External event logging may also be disabled. You can re-enable them on the console System Configuration page Advanced Options and Events tabs, respectively.
- If the database you want to restore or reconnect to is a SQL Server 2005 Express database, contact Bit9 Support before continuing.
- If you are restoring from or reconnecting to a Parity 7.0.0 or greater database, and if you imported one or more certificates as part of your original Bit9 installation, those certificates are available in the database, and you can use them when you restore or reconnect. You will need the password for each certificate to reuse them.
- If you are upgrading from a previous version of the Bit9 Server, see section [“Upgrading from a Previous Bit9 Version”](#) on page 50 instead of this section. You may also receive supplemental field upgrade instructions from your Bit9 Support representative.
- During Bit9 Server installation, you will have a choice to use Windows authentication or SQL authentication to configure access to the SQL Server by the Bit9 Server. For either method, the account you use to access the database must be added to SQL Server with “sysadmin” checked in the Server Roles.
- Although not common, if you left a Bit9 Agent on the system on which you are installing the Bit9 Server, that agent could block installation of the new server. In this case, you will be prompted to remediate the blocking conditions. If you are prompted to disable tamper protection, you must have the client management access password or user account you provided during the previous server installation or configuration.

To install the Bit9 Server and reconnect to or restore a backup of a database:

1. Log in using an account with local Windows administrator credentials. If you plan to use Windows Authentication to login to a remote Bit9 database, install the Bit9 Server logged in with an account that has been added to SQL Server with “sysadmin” checked in the Server Roles. Bit9 strongly encourages using a specific Domain account for installing and logging in to the Bit9 Server, and for database access, to simplify control of both database and Active Directory permissions.

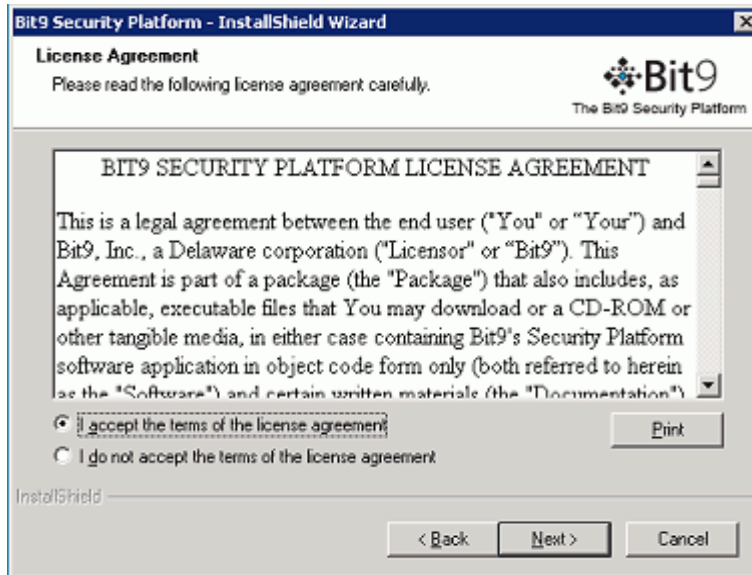
Important

Do not change the privileges of the account used to install the Bit9 Server after installation. This account must continue to have local administrator privileges for the Bit9 Server to function properly, and will also be used for server upgrades.

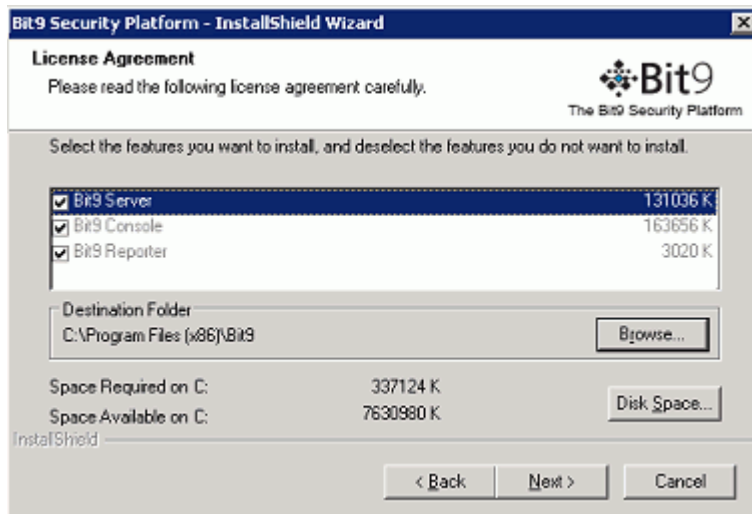
2. Make the Bit9 Server installation file available to the installation computer (either by download or inserting media in an accessible location).
3. Run the installer in either of the following ways:
 - a. To install on a local server, double-click the `ParityServerSetup.exe` file to start the installation program. Continue to the next step.
 - b. To install from a remote desktop, copy the `ParityServerSetup.exe` file to the installation computer and execute the file. Continue to the next step.



4. From the Welcome page, click **Next**. The License Agreement screen appears.

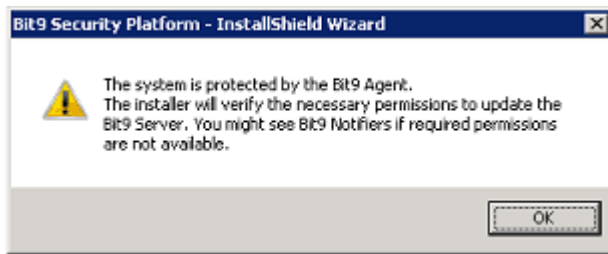


5. Review the Bit9 Security Platform software license agreement. You must agree to the license terms to install the Bit9 Server. When you click the **I accept** button and continue, you agree to all terms of use. To continue, click the **Next** button. The Select Features dialog appears.



- a. Although they have checkboxes, Bit9 Console, Bit9 Server, and Bit9 Reporter are always installed — they cannot be deselected. The Bit9 Console is the web interface to the Bit9 Server. Bit9 Reporter is the service that connects the Bit9 Server to the Bit9 Software Reputation Service, which provides access to a database of file information. Reporter, which runs as a Windows service, also provides essential reporting capabilities for the Bit9 Server.
- b. Either keep the default installation folder (which differs from 32-bit to 64-bit systems) or click **Browse** and navigate to the folder in which you want to install the Bit9 Server. If you don't choose the default, use a path that has only valid ASCII characters, not Unicode. When you have chosen the folder, click **Next**.

6. At this point, the installation program checks that the server environment meets the requirement for Bit9 Server installation. If no issues are found, you will not see any additional dialogs, and the Database Server screen will appear (step 8). Warning dialogs appear under the following conditions:
 - a. If files are detected in the installation directory, you will see a warning dialog. You can continue the installation without removing the files, but should examine the files to see whether you want to copy and/or remove them. In most cases, these will be log files from Bit9 Connector appliances or services.
 - b. If Bit9 Agent is detected on the Bit9 Server computer, you will see the following dialog:



If this dialog appears, click **OK** to dismiss it and initiate the system check that determines whether the agent and/or other factors would prevent successful installation of the server.

- c. If the system check finds any issues that would prevent server installation from completing, you will see a dialog box describing issues that need to be resolved before you can proceed. If this dialog appears, use the information in it to change the appropriate settings and then click **Next** (you do not need to exit the installation while you remediate the problems). When you click Next, the system check is run again, and if all issues are remedied, the installation moves to the next step. If there are still outstanding issues, those issues will be listed again and you will have another opportunity to correct them. If necessary, you can click **Cancel** to exit the installation dialogs.

Note that if you are prompted to disable tamper protection, you must have the client management access password or user account you provided during the previous server installation or configuration. In the reconnect/restore case, you will not be able to use the Bit9 Console to disable tamper protection.

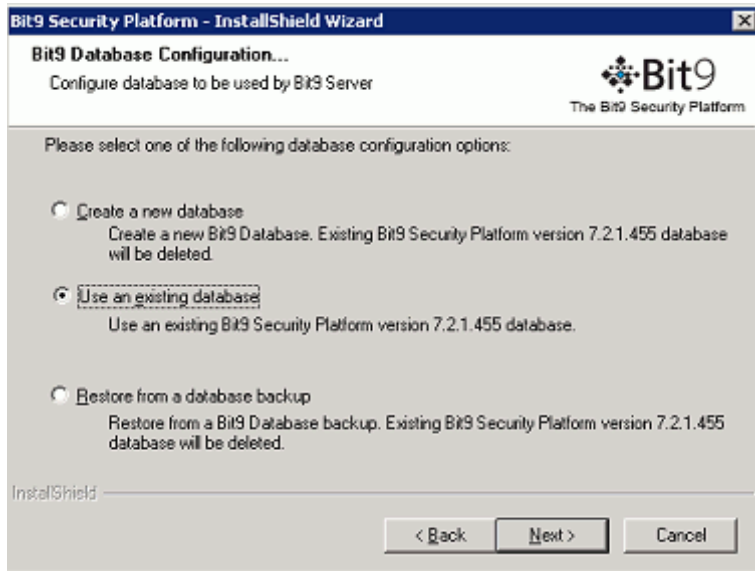
7. The Database Server screen appears next. This screen includes two configuration choices:

The screenshot shows the 'Database Server' screen of the 'Bit9 Security Platform - InstallShield Wizard'. The window title is 'Bit9 Security Platform - InstallShield Wizard'. The main heading is 'Database Server' with the instruction 'Select database server and authentication method.' The Bit9 logo and 'The Bit9 Security Platform' text are in the top right. The instructions state: 'Select the database server from the list below or click Browse to see a list of all database servers. You can also specify the way to authenticate your login using your current credentials or a SQL Login ID and Password.' There is a 'Database Server:' label above a text box containing '[local]' and a 'Browse...' button to its right. Below this, the 'Connect using:' section has two radio buttons: 'Windows authentication' (selected) and 'SQL Server authentication using the Login ID and password below'. Under the SQL option, there are 'Login ID:' and 'Password:' labels above their respective text boxes. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons. The 'InstallShield' logo is in the bottom left corner.

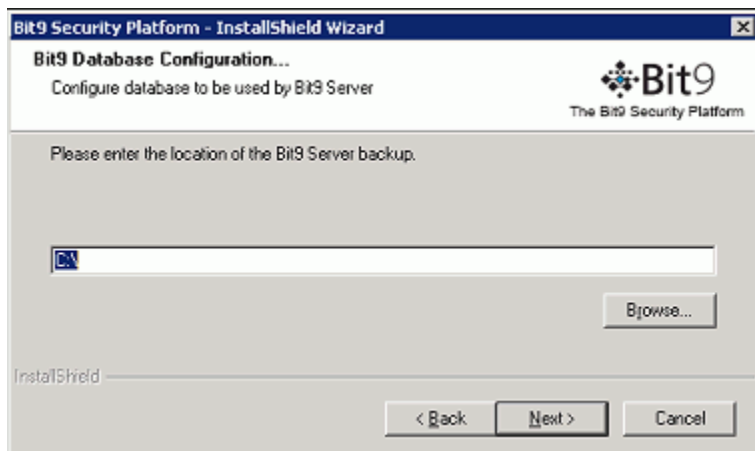
- a. Database Server is the name of the SQL server, and optionally, its instance. Enter the server name and instance name (if any) you use to connect to the server. If the database server is local, you will be able to reconnect, and if necessary, restore from backup files you have on the server. If the database server is remote, you will be able to reconnect only.
- b. With the Connect Using radio buttons, choose Windows Authentication (i.e., authenticate with the user doing the Bit9 Server installation) or SQL Server Authentication. If you choose SQL Server Authentication, provide the Login ID and Password. Your choice here determines how access to the SQL Server by the Bit9 Server will be authenticated, both during and after the Bit9 Server installation.
- c. When you are finished entering database information, click **Next**.

Note: For either authentication method, the user must have been given the “sysadmin” Server Role in SQL Server.

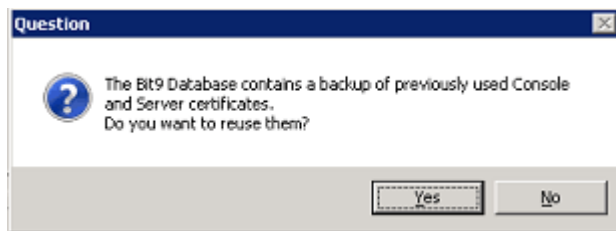
8. The Bit9 Database Configuration Options screen appears. The options on the screen depend upon whether a Bit9 database was detected at the location you provided on the previous screen:



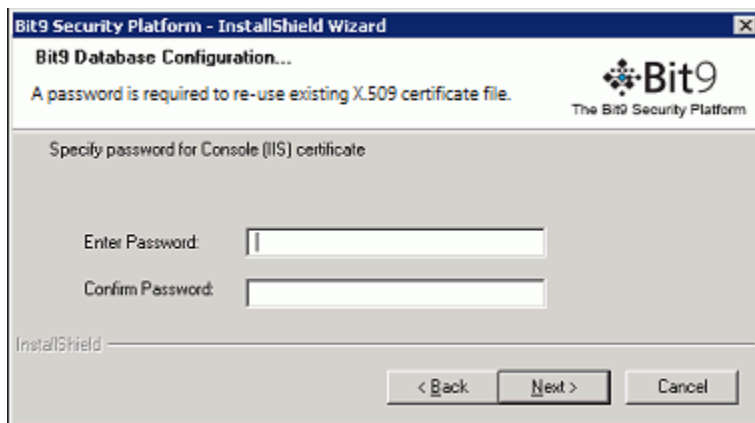
- a. If the installation program detects a usable Bit9 database, your choices are to create a new Bit9 database (and delete the existing database) or use an existing Bit9 database and upgrade it to 7.2.1. Choose **Use an existing database** to preserve your Bit9 data and upgrade the database, and then click **Next**. If you choose this option, a warning appears reminding you to backup your Bit9 database before proceeding. If you have recent backups, click **Yes** to continue, and skip to step 12.
 - b. If the database location you provided is local, the **Restore from a database backup** option is enabled. Choose this option to restore your previous database from a backup file, and click **Next** to continue.
9. If you chose **Restore from a database backup**, the Bit9 Server Backup Restoration screen appears.



10. On the Backup Restoration screen, enter the path to the folder containing the backup database, or use the **Browse** button to locate it. Click **Next**. The Bit9 Server Backup Information screen appears.
11. Examine the information on the Bit9 Server Backup Information screen. Note that if you are restoring from a backup from a previous version of Bit9, that database will be updated to the version matching your installer if you proceed. Use the **Back** button if you want to use a backup other than the one described on this screen.
12. When the information on the Bit9 Server Backup Information screen is correct and you want to proceed, click **Next**. If there are certificates stored in the database, you are prompted to decide whether to re-use any stored certificates. The dialog will specify whether there is a console certificate only or certificates for both the console and the server.



13. If you want to re-use the certificate(s), click **Yes** in the dialog.
 - If you are restoring a database from backup, you will be prompted for the certificate passwords *after* the database is restored.
 - If you are reconnecting to a database, the Restore Pre-Existing X.509 Certificate for the Bit9 Console screen appears.



14. The database can contain either one or two certificate files, and there will be a dialog for each one found. Enter a password and click **Next** in each dialog.

Note: By default, the verified password from the first dialog will be pre-populated in the second dialog (if there is one). If there is a password problem, an error message will indicate that immediately and give you the chance to re-enter the password. If a valid password is provided but another certificate restoration problem occurs during the installation, an error message will appear and a self-signed certificate will be generated instead so that installation may continue.

15. After you complete the certificate dialogs, the Logon Information screen appears. On this screen, choose the logon account to be used by the Bit9 Server. You can choose one of two modes of logging in:

The screenshot shows a Windows-style dialog box titled "Bit9 Security Platform - InstallShield Wizard". The main heading is "Logon Bit9 Server As..." with a subtitle "Specify the user account to be used by Bit9 Server". The Bit9 logo and "The Bit9 Security Platform" text are in the top right. A note states: "Specify the user account to be used by Bit9 Server. The user account must be in the format 'DOMAIN\Username' and must have access to the SQL database server." There are two radio buttons: "Local System Account" (selected) and "Specify Account". Below "Specify Account" are fields for "User name:" (containing "bit9srv\administrator") and "Password:". At the bottom left is the "InstallShield" logo, and at the bottom right are "< Back", "Next >", and "Cancel" buttons.

- a. The Local System Account radio button instructs the installation to configure the Bit9 Server to use the built-in Windows system account.
- b. The Specify Account radio button activates the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username and have full access to the SQL database server. The default for this choice is the currently logged in user.

Note

- Bit9 strongly encourages using a specific Domain account and the Specific Account option to simplify control of both database and Active Directory permissions. In general, the installer should be run by this same Domain account.
- In Bit9 Security Platform 7.2.1, an SSL certificate is automatically generated to protect communications between the Bit9 Server and its agents. If the Common name of the server does not match the configured server name, then server and agents will be unable to communicate correctly.
- For local SQL Server Express databases, the currently logged in user must be the same as the user specified in the Login Account installation dialog. If you attempt to enter a different user, an error message appears and you must re-enter the current user. The logged in user must have been given the “sysadmin” Server Role in SQL Server.
- In the case of remote databases, the installation program cannot confirm the validity of the account you provide. Note that if you provide an invalid login account, Bit9 Server installation will be unsuccessful and you will need to reinstall.

16. When you have provided logon information, click **Next**. The Server Configuration Options screen appears.

The screenshot shows a Windows-style dialog box titled "Bit9 Security Platform - InstallShield Wizard". The main heading is "Server Configuration Options" with a subtitle "The following information is needed to configure the server". The Bit9 logo and "The Bit9 Security Platform" text are in the top right. The instruction "Please enter the information you would like your Bit9 Agents to use when connecting to the Bit9 Server." is at the top. Below are three input fields: "Server Address:" with the value "bit9srv.mycorp.local", "Console Port:" with the value "41001", and "Agent Port:" with the value "41002". A paragraph of text explains that Bit9 Agents use secure SSL communication using the X.509 certificate generated by the Bit9 Server, and that after installation, an existing certificate can be substituted via the Security tab in the Administration > System Configuration page. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is in the bottom left corner.

17. From the Server Configuration Options screen, review the configuration settings. In the Server Address field, the preferred address is a fully qualified DNS name (or alias) that is resolvable by all computers running Bit9 Agent. Although not recommended, if the server is assigned a static IP address that will not change at reboot time, you can keep the default IP address selected for the Bit9 Server. The installation program automatically supplies the correct information for the installation machine. Console Port, which is used for communications between the Bit9 Server and its user interface, is **41001**. Agent Port, which is used for communication with Bit9 Agents, is **41002**.

Note

- Bit9 strongly recommends the use of a fully qualified DNS name for Server Address whenever possible. Use of a CNAME (alias) may provide even more flexibility and reliability.
- If you use multiple NICs, make sure the FQDN you use in the Server Configuration screen refers to the address of the card(s) you want the Bit9 Agents to connect to.
- If you are reconnecting to an existing Bit9 database, and you enter a Server Address other than the one you used previously, a dialog box appears asking you to choose one of the two addresses. If the new address you provided is actually a different server, click **Yes** to modify the database with the new name. If the new address you provided is an *alias* for the address currently in the database, click **No** to use the existing address from the database. Note that if you use the new address (i.e., click **Yes**), any existing Bit9 Agents will not be able to reconnect to the server unless you provide a DNS alias between the new and old names. If you are not sure which to choose or you made an error in entering the name, click **Cancel** to return to the configuration screen.

18. If you chose Specify an Account in the (Bit9 Server) Logon Information screen (step 12), another Logon Information screen appears next, for the Bit9 Console (under IIS). Otherwise, go to step 19.

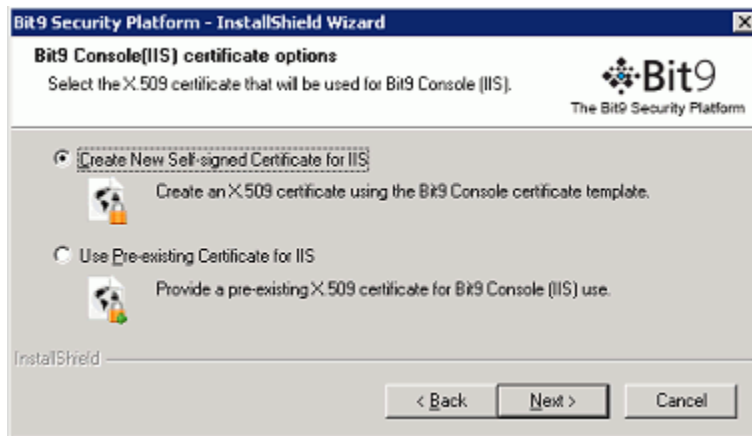
This screen allows you to specify a different logon for the Bit9 Console, the web-based user interface for the Bit9 Server.

- a. Choose **Local System Account** to configure the Bit9 Server to use the built-in Windows system account for Bit9 Console logons.
- b. Choose **Specify Account** to activate the Username and Password fields so that you can provide account information. As the screen notes, the account you provide must be in the format DOMAIN\Username.

Note

If you use a logon other than the current user, a warning dialog will be shown: “The Bit9 Server installer is unable to validate whether the specified account is able to access the SQL database server. Are you sure you want to continue?” If you are certain the account you provided is valid, choose **Yes**.

- c. When you have provided Bit9 Console logon information, click **Next**. If you restored certificates in a previous step, skip to step 22.
19. If there were no certificates stored in the database, or if you chose not to restore them in a previous step, the Certificate Options screen appears. From the Certificate Options screen, choose the digital certificate that will appear to Bit9 Console users. You either create a certificate using a template provided by Bit9 or substitute your company’s certificate.



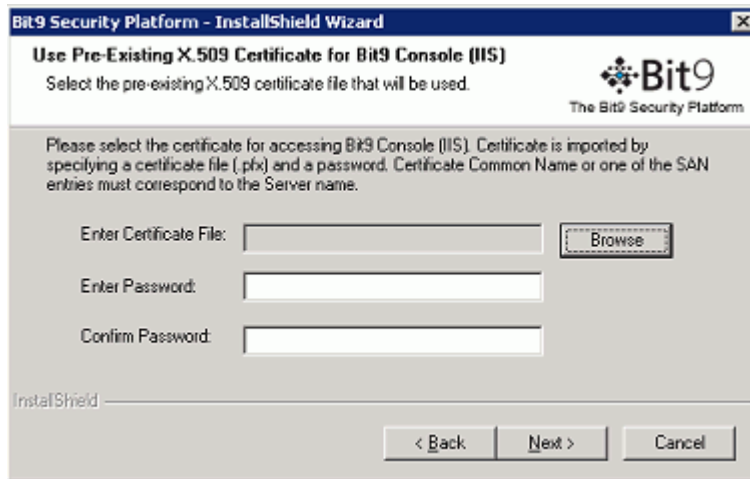
- a. If you do not have your own certificate, choose **Create Certificate**. This allows you to create a Bit9 self-signed certificate. Self-signed certificates will generate warning boxes when you log in to Bit9 Console using Internet Explorer or Firefox, although Firefox will allow you to permanently accept the certificate to eliminate future warnings. To create a certificate, choose **Create Certificate**, click the **Next** button, and skip to Step 20.
- b. To substitute your own certificate, choose **Use Pre-existing Certificate**, click the **Next** button, and skip to Step 21.

20. If you chose Create Certificate, the Create X.509 Certificate screen appears.

- a. By default, all certificate details correspond to Bit9 name and address data. Please replace them with details of your company. The default password is 'password'. Bit9 recommends that you change it, and keep a record of your new password so it can be retrieved for later use. The Common Name field defaults to the IP Address or DNS Name of the Bit9 Server; it cannot be changed. If the Bit9 Server is reachable by multiple DNS names, you can use the Subject Alternate Name field to specify the alternate names.

When the certificate is validated against a computer, it is validated against the Common Name or one of the Subject Alternative Name entries (if they exist). If both are present, names in the Subject Alternative Name field have priority.

- b. When the information you want is in all fields, click **Next** to create the certificate and skip to step 22.
21. If you chose Use Pre-existing Certificate, the Use Pre-existing X.509 Certificate screen appears. Enter the required information:



Bit9 Security Platform - InstallShield Wizard

Use Pre-Existing X.509 Certificate for Bit9 Console (IIS)
Select the pre-existing X.509 certificate file that will be used.

Please select the certificate for accessing Bit9 Console (IIS). Certificate is imported by specifying a certificate file (.pfx) and a password. Certificate Common Name or one of the SAN entries must correspond to the Server name.

Enter Certificate File:

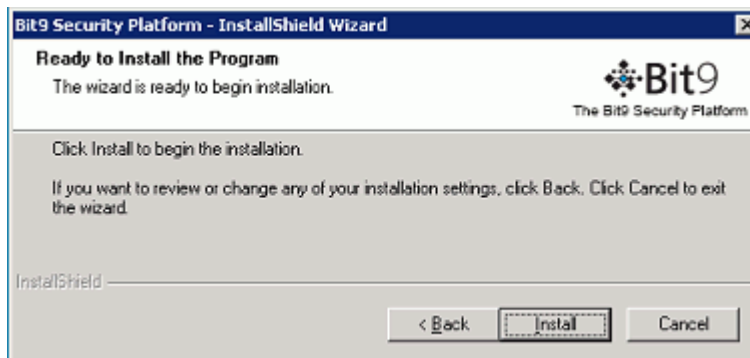
Enter Password:

Confirm Password:

InstallShield

< Back **Next >** Cancel

- a. Click the **Browse** button next to the Enter certificate file field, navigate to the PFX (PKCS.12) certificate file you want to use, and click **Open** when you have located the file. The filename appears in the certificate file box.
 - b. Enter the password for the certificate, and re-enter it in the confirmation field.
 - c. When you have entered the certificate file and the password, click **Next**. The Ready to Install screen appears.
22. If you are satisfied with your installation choices, click the **Install** button.



Bit9 Security Platform - InstallShield Wizard

Ready to Install the Program
The wizard is ready to begin installation.

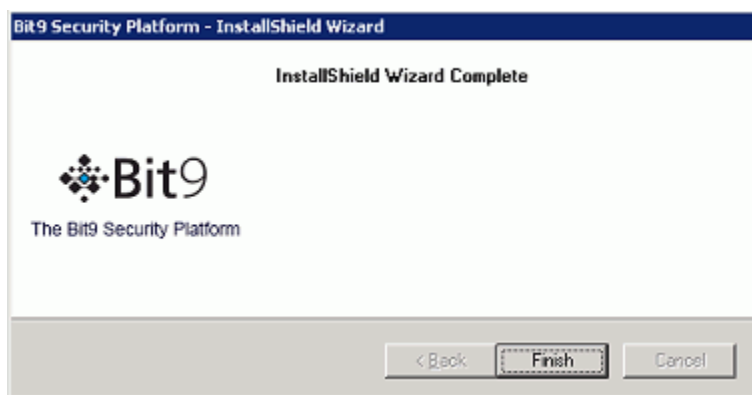
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

< Back **Install** Cancel

23. Bit9 Server installation commences, and an installation status bar shows progress. When the InstallShield Wizard Complete screen appears, the installation is complete.
- In some cases, you will need to restart the server computer after installation is completed, and the dialog will include an option to restart now. Choose to restart now unless you need to complete some other activity on this computer.
 - Click the **Finish** button. Bit9 Server, which runs as a service, begins to operate after you click this button. Installation logs are placed in the Bit9 installation folder (for example, *C:\Program Files (x86)\Bit9*).



Upgrading from a Previous Bit9 Version

Upgrading to Bit9 Security Platform 7.2.1 requires that your existing server be at the latest patch of version 6.0.2 or a supported 7.0.0 or 7.0.1 patch. See the *Release Notes* for this release for detailed information about build and patch numbers from which you can upgrade.

Upgrades from pre-6.0.2 Parity versions are not supported by the installation program, but Bit9 Support can help you make a transition from an earlier version.

Important

You must backup the Bit9 database before running an upgrade. Some database upgrade failures are non-recoverable. Be sure you have a backup no more than one day old.

Dialogs during the Bit9 upgrade process will warn you if your database backup is not recent (or its status cannot be determined). Proceeding in these cases is not recommended.

In addition to backing up your server, you should consider the following requirements and recommendations before performing an upgrade:

- Changing the Bit9 Server name at upgrade is not recommended, especially if you use your own distribution methods to upgrade Bit9 Agents. Consider using a CNAME for the Bit9 Server to avoid having to change the name.
- Bit9 Server upgrades must be run as the Bit9 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 the Bit9 Server must be used (either by login or runas) to install the upgrade.
- Do not use the Bit9 Server installer program (ParityServerSetup.exe) to upgrade the Bit9 Server from one build to another within the same version (e.g., from 7.2.1.542 to 7.2.1.829). Running the full installer in a build-to-build upgrade removes the current Bit9 instance instead of upgrading it. For build-to-build upgrades, there is a separate "patch" installation procedure. Apply the patch to the server according to the instructions you received with it, and then update Bit9 Agents as described in the "Managing Computers" chapter of the *Using the Bit9 Security Platform* guide (or online help).
If you inadvertently run the full installer for the build-to-build case, run it again, and, when prompted, select 'Use the existing database').
- If you are upgrading the Bit9 Server on a system that is protected by Bit9 Agent, examine any custom rules that protect the Bit9 installation folder and its subfolder. These should be disabled prior to installing the upgrade and re-enabled after the upgrade is complete. The upgrade installation program will warn you if a Bit9 rule or third-party software is blocking access to a folder or registry location that the Bit9 Server installer must access to complete the upgrade.

It is also possible, although uncommon, that you will be prompted during installation to disable tamper protection on the server's agent. In this case, be certain to re-enable tamper protection as soon as the server upgrade is completed, and do not disable tamper protection unless prompted.

Upgrade Installation Overview

Upgrading to Bit9 Security Platform version 7.2.1 involves the following high-level steps, most of which are described in more detail later in this section:

- Read through the separate *Operating Environment Requirements* document for the current distribution of Bit9 Security Platform version 7.2.1 to be sure your server platform meets the current hardware and software requirements for this release.
- Read through this upgrade section to get a full overview of the upgrade process.
- Contact Bit9 Technical Support (support@bit9.com or 877-248-9098) for any recent changes to upgrade procedures, or for advice on special cases, including strategies for getting to version 7.2 from a pre-6.0.2 version of Bit9 Parity and what to do if you are currently running a Bit9-installed version of SQL Server Express.
- Backup the Bit9 Server database. Do not proceed with the upgrade without a recent backup since database upgrade failures are non-reversible.
- Disable third-party Bit9 Agent deployment mechanisms (such as SCCM).
- Stop any other activity (including backup jobs) or user access on the SQL Server.
- Either log in as the Bit9 service user account that was configured during Bit9 Server installation or use *runas* that user to install the upgrade.
- For upgrades to a different *version* number (e.g., from 6.0.2 or 7.0.1 to 7.2.1) run the Bit9 Server installation (**ParityServerSetup.exe**). For build-to-build upgrades (e.g., 7.2.1.456 to 7.2.1.845), use the patch installation procedure, which does not require the steps in this document. Patch releases are accompanied by Release Notes describing any special considerations.
- Wait for automatic post-installation server updates to complete.
- Make any needed System Configuration changes to the Bit9 Server.
- If you distribute agents using your own deployment mechanism, upgrade Bit9 Agent distribution points and re-enable deployment mechanisms.
- If you upgrade agents using the Bit9 Server, re-enable the Bit9 Server's upgrade features.

Important

When the 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 Bit9-managed computers. These upgrades may also require a new inventory of files in any trusted directories to determine whether there are previously ignored files that are now considered interesting. For some upgrades, this process can involve activity similar to agent initialization, and may cause considerable input/output activity. This could take less than an hour or last for many hours, depending on the number of agents and files.

For both Bit9-managed upgrades and third-party distribution methods, Bit9 recommends a phased upgrade of agents to avoid an unacceptable impact on network and server performance.

See the “Managing Computers” chapter in the *Using the Bit9 Security Platform* guide for full agent installation and upgrade procedures.

- If you have used External Events Logging in a pre-7.0 version of Bit9 Parity, update the database by running **external_events.sql** on the SQL Server after you upgrade the Bit9 Server. Depending upon database size, this script could run for a considerable amount of time before completion.
- For agent upgrades, reboot on systems that prompt you to do so. This should only be necessary for certain systems running Windows XP or Windows 2003.
- If you have used Syslog/SIEM integrations with Bit9, such as QRadar or ArcSight, make sure to consult the *Bit9 Events Integration Guide* for Bit9 Security Platform 7.2.1 to prepare your configuration for required changes. Note that integrations with SPC and SMP integrations are not supported in Bit9 Security Platform 7.2.1

Note

- You cannot upgrade Bit9 Agents running on Windows 2000 systems. You can continue to run v6.0.2 agents on those systems, but they will not have full v7.2.1 functionality and will have limited support.
- Changing the Bit9 Server name at upgrade is not recommended, especially if you use your own distribution methods to upgrade Bit9 Agents. Consider using a CNAME for the Bit9 Server to avoid changing the configured name in Bit9.

Upgrade Pre-installation Requirements

Your existing Bit9 Server must be at least at the v6.0.2 level to be upgradable to 7.2.1. Also, all agents on all systems you plan to use with version 7.2.1 should be at version 7.0.0, 7.0.1 or the latest 6.0.2 patch. See the “Managing Computers” chapter in the *Using the Bit9 Security Platform* guide (or Bit9 Console help) for details on agent upgrades.

Backup the Bit9 Server

Bit9 requires that you backup the Bit9 Server *before* running the Bit9 Server installer for an upgrade. Some failures of the database portion of the server upgrade are non-recoverable, and if you haven’t backed up recently, you will lose data.

Bit9 recommends that you use your own backup mechanism to back up the Bit9 database. However, if you have not backed up the database and need to use the Bit9 mechanism, go to the Advance Options tab on the Bit9 Console System Configuration page and enable backups.

Important

System Backup does not backup IIS certificates. Also, pre-7.0 versions of the Bit9 Parity Server do not backup the certificates configured for the server. Please do a separate backup of IIS certificates, and if upgrading from 6.0.2 (or via 6.0.2 from an earlier release), all Bit9 Server and Console certificates, on a system other than the Bit9 Server.

Disable Software Deployment Mechanisms

Please disable any software deployment mechanisms, such as SCCM, used to distribute Bit9 Agent until after the upgrade completes and you have had an opportunity to update their respective distribution points with the upgraded Bit9 Agent installers.

Stop SQL Background Jobs

Because the Bit9 database is updated during a server upgrade, no other database jobs should be running. This includes background jobs such as database maintenance and backup activity. Stop all of these jobs, and confirm that no one else is using the database before initiating the Bit9 Server upgrade.

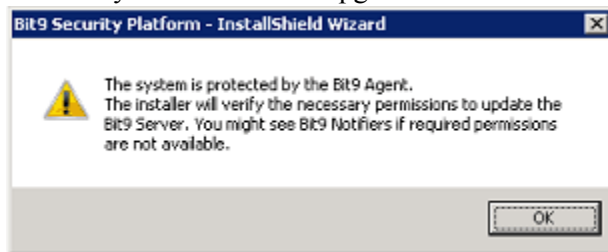
Run the Bit9 Server Upgrade Installation

Make the Bit9 Server 7.2 or downloaded installer files available to your Bit9 Server. If you have a CD and no physical CD drive is present on the Bit9 Server, you can insert the CD in another machine, “share” the drive and mount that “share” from the Bit9 Server machine. Launch the **ParityServerSetup.exe** application to validate and upgrade the Bit9 Server components.

Upgrade Installation Checks

The upgrade installation program checks that the server environment meets the requirements for Bit9 Server installation. There are two important checks that might produce warnings after you initiate the upgrade:

- **Blocked Access Warning** – If the Bit9 Agent is installed on the system, a dialog box appears reporting that the installer will check to confirm that it has access to the necessary locations for an upgrade.



If the system check finds that Bit9 Agent or any other system software is blocking access to folders or registry locations needed by the installer, the issues will be listed in a dialog, and you will have the opportunity to remedy them and continue with the upgrade. When you correct the issues listed, click the **Next** button on the dialog to run the system check again and (if all issues are corrected) proceed with the upgrade.

It is possible, although uncommon, that you will be prompted during installation to disable tamper protection on the server’s agent. In this case, be certain to re-enable tamper protection as soon as the server upgrade is completed, and do not disable tamper protection unless prompted.

- **Bit9 Detection Downgrade Warning** – Bit9 Security Platform v7.2.1 includes Bit9 Detection v1.2. If the Bit9 Server upgrade installer finds that your current server and database include a later version of the advanced detection features, it will display a dialog allowing you to continue installation (and temporarily revert to Detection v1.2) or cancel the installation. Detection can be upgraded to the latest version after the server upgrade is completed.

- **Database Backup Warnings** – Bit9 Server upgrades include updates to your Bit9 database. Some situations can cause failure of the database update scripts, and some of these failures are unrecoverable. You must backup your database before an upgrade to make sure you can restore your most recent data. The Bit9 upgrade installer checks to see whether a recent backup can be found, and displays different dialogs depending upon what is found:
 - In all cases, an informational dialog is displayed warning that a recent database backup is required.
 - If the installer determines that there is no recent backup, it will display a dialog telling you to do a backup before proceeding.
 - If the installer is unable to determine when the most recent backup was, it will display a dialog telling you to check the date of the backup before proceeding.You have the option of cancelling the upgrade or continuing after these warnings. Continuing without a recent backup is *not recommended*.
- **Database Size Warning** – Bit9 Server upgrades can require a considerable amount of free storage space for the database. The installer attempts to confirm that there is enough space available for a database upgrade, and displays a dialog in these cases:
 - If it cannot determine whether there is enough space (for example, because it does not have privileges to view a remote database), it will display a dialog with the current database size, the estimated amount needed for an upgrade, and a recommendation to make sure there is enough space available.
 - If the installer can determine the free space available and determines that it is insufficient, it will display a dialog with the current and required amount of free space, and a warning that there is not enough space.



You have the option of continuing after either of these warnings, with or without remediating space issues. If the upgrade is continued and there really is not enough space, the upgrade program will exit and revert to the previous database and Bit9 Security Platform version.

- **SQL Server Express** – If you are using SQL Server Express for your existing Bit9 Parity database and your database is larger than 4Gb, the upgrade installer will detect this and a dialog will warn you that your database may become unusable upon upgrade. You will have the option of continuing the upgrade, but you should consider upgrading to a full version of SQL Server, as specified in the *Operating Environment Requirements* for this release. SQL Server Express has a firm limit on the database size, and if you see this warning, you are almost certain to exceed that limit.
- **Bit9 Connector for Check Point Password** -- If a previous installation of Bit9 Server used specific credentials during server installation, you may see a message indicating that Bit9 services could not be started due to the Bit9 Connector for Check

Point service. In this case, you will be prompted for the Bit9 Connector Check Point credentials.

- **Database Update Failure** – If there is a failure in the database update portion of the server upgrade, different dialogs will be displayed depending upon the location of the failure. If the failure is potentially recoverable, you will be given the option of continuing. If it is not recoverable, you will see a message ending the upgrade and listing recommended steps.

Upgrade Completion

After the installer finishes and exits, the Bit9 Server starts running again and updates the existing agent installers for each policy and platform. This process takes a few minutes, the exact time depending upon the number of policies you have. If you are refreshing the version of the Bit9 Agent installer on distribution points for a software deployment mechanism, make sure the agent installer has completed the upgrade to 7.2.1.

Note

In pre-7.0 releases of Parity, if IPv6 was configured on the server system, the Parity installation reverted it to IPv4 because IPv6 was not supported. In Parity 7.0.0 and later, IPv6 is supported. During an upgrade, if a system was changed to IPv4 during a previous installation, a dialog appears allowing you to return to IPv6 defaults. If you choose this option, future upgrades will maintain the IPv6 address option. This option requires a system reboot, which will be initiated by the Bit9 Server installer.

Review Post-Upgrade Server Configuration

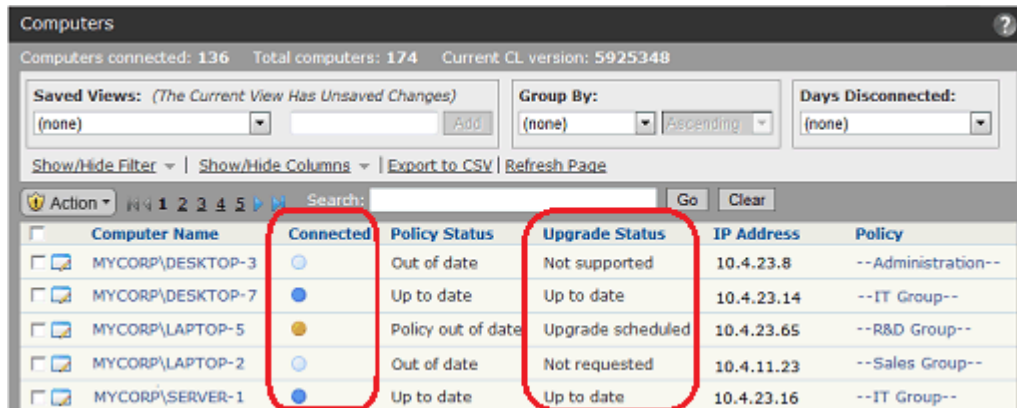
After you run the Bit9 Server upgrade installation, complete the following checklist prior to upgrading agents:

- In the **Rules > Software Rules** section of the Bit9 Console, review **Updaters** as necessary (e.g., to see any new updater versions or new updaters).
- In the **Rules > Software Rules** section of the Bit9 Console, if you upgraded the Bit9 Server on a system that is protected by Bit9 Agent, and you disabled certain **Custom** rules to allow the upgrade to run, re-enable those rules.
- In the **Assets > Computers** section of the Bit9 Console, if you disabled tamper protection on the server's agent during upgrade, open the Computer Details page for that agent and re-enable tamper protection.
- In the **Administration > System Configuration** section of the Bit9 Console, go to the **Advanced Options** tab, and modify the **Database Backup** configuration if necessary. Then re-enable backup.
- If you plan to use Reputation Approvals, it is better to enable it as soon as possible to avoid heavy network traffic later. This feature requires that you have Bit9 Software Reputation Service enabled (**Administration > System Configuration > Licensing**). If you have it enabled, to access this feature, choose **Rules > Software Rules** on the console menu and click the **Reputation** tab. See "Reputation Approvals" in the *Using the Bit9 Security Platform* guide for more information.
- Automatic Agent Upgrade is disabled in the server upgrade process. To re-enable:

- Be sure that you have configured the policies you want to upgrade first for automatic upgrade, and those you don't need upgraded right away not to upgrade. Upgrading large numbers of agents at once can create a large load on the server.
- In the **Administration > System Configuration** section of the Bit9 Console, choose the **Advanced Options** tab and re-enable automatic upgrades of Bit9 Agents.
- Automatic backup is disabled if the Bit9 database was restored during the upgrade. If you use automatic backup and want to re-enable it, see "Backing Up the Bit9 Server" in the Bit9 Console help.
- If you installed the optional Bit9 Detection Enhancement on v7.0.0 or v7.0.1, review the following after the server upgrade and take action as needed:
 - Bit9 Security Platform v7.2.1 includes Bit9 Detection v1.2. It is possible that you have a later version of detection installed on your current Bit9 Server. If your Bit9 Server has Bit9 Software Reputation Service (formerly Parity Knowledge Service) enabled and connected to the server, the "Indicator Sets" containing the latest threat indicators will be downloaded by your server automatically not long after the server upgrade is completed. Otherwise, you can download the detection upgrade setup program from the Bit9 Support web site.
 - The threat indicators that were formerly grouped as Updaters in pre-7.2.0 versions were moved to separate Indicator Sets beginning in v7.2.0, and are disabled after an upgrade. If you are upgrading from a pre-7.2.0 release, to re-enable threat indicators, choose **Rules > Indicator Sets**, check the box next to each Indicator Set you want to enable, and choose **Enable Indicator Sets** on the Action menu. Do this whether or not you update the indicator sets. See "Advanced Threat Detection" in the online console Help or PDF version of the *Using the Bit9 Security Platform* guide for more information.
- If you use a third-party software distribution system to install Bit9 Agents, re-enable the distribution system and update the distribution points as the next section specifies.
- For upgrades from pre-7.0 releases, the server will not export any new events to an external database until the schema is upgraded manually. If you have used External Event Logging in pre-7.0 releases, update the external events database after you finish the Bit9 Server upgrade installation.
 - Navigate to the **sql** folder in the Bit9 Server installation folder (for example, *c:\Program Files (x86)\Bit9\Parity Server\sql*) and copy **external_events.sql** to your remote database server.
 - On the database computer, use Management Studio to run **external_events.sql** on the Bit9 database. Note that the time required for the script to complete the update can be considerable, depending upon the size of your database.
- If you have used the Live Inventory SDK, review Appendix A of the *Using the Bit9 Security Platform* guide to see whether any of the fields you used have changed.
- Bit9 Platform v7.2.1 includes a System Health feature that monitors a variety of factors, including compliance of your system with the Bit9 *Operating Environment Requirements*. The indicators for this feature must be downloaded via the Bit9 Software Reputation Service. See the *Using the Bit9 Platform* guide or online help in the console for more information about enabling this feature.

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.



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 | 1 2 3 4 5 | Search: | Go | Clear

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.

See the “Managing Computers” chapter in the *Using the Bit9 Security Platform* guide (or online help) for addition information about automatic and manual agent upgrades, and about monitoring upgrade status.

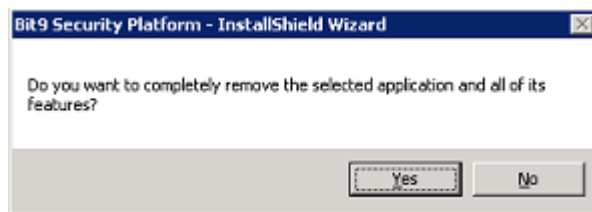
Uninstalling the Bit9 Server Software

The server uninstallation program removes Bit9 files and associated third-party software installed on the system. To uninstall the Bit9 Server, you must log in as a user with administrative privileges, preferably as the same Bit9 service user that was used to install Bit9 Server. The uninstall program is on the **Start > All Programs > Bit9** menu, although you can also use the **Add or Remove Programs** interface in the Windows Control Panel. Consider the following points before you uninstall:

- If you are uninstalling and do not intend to reinstall the Bit9 Server, place all policies in Disabled mode before uninstalling. Otherwise, computer users will not be able to uninstall the agent without special assistance. If you attempted to uninstall the Bit9 Server without changing all policies to Disabled mode first, contact Bit9 support.
- When you start the Bit9 Server installer/uninstaller program, it verifies that you have the permissions required to uninstall the Bit9 Server. If there are any rules or permissions prevent un-installation from going forward, the installer provides a report detailing what must be done before you can proceed. This includes blocks due to an enabled Bit9 Agent on the computer running the Bit9 Server and other folder or registry permission issues.
- Self-signed Bit9 certificates are removed during the uninstallation process. If you used a certificate from a certificate authority (i.e., one that is installed in the Windows Certificate Store), it is not removed.

To uninstall the Bit9 Server software:

1. Either go to the Control Panel and click **Bit9 Server** on the Remove Programs list, or on the Windows Start menu, choose **All Programs > Bit9 > Uninstall Bit9 Server**. A confirmation dialog appears.



2. Click the **Yes** button to start the uninstallation process. When the uninstallation process is complete, either the dialog will close by itself or you will see the Uninstall Complete screen.
3. Generally, you do not need to reboot your system after uninstalling the Bit9 Server. If a reboot is necessary (which is true only if the uninstall program could not remove certain Bit9 files), the screen includes reboot options.



If the options appear, rebooting now is recommended unless you have other immediately necessary activity on the server (for example, an error in uninstalling).

- a. Choose a reboot option if prompted.
- b. Click **Finish**.

Notes

- For instructions on uninstalling the Bit9 Agent, refer to the *Using the Bit9 Security Platform* guide or online Help system.
- Uninstalling the Bit9 Server reverts the IIS configuration to its state prior to Bit9 Server installation. Any configuration changes applied during the time the Bit9 Server was installed are lost.
- The Bit9 Server uninstall program will *not* remove the Bit9 database. It must be deleted separately.
- If the FastCGI module was installed by the Bit9 Server, the uninstall program presents a choice to un-install it or leave it installed once the Bit9 Server itself has been uninstalled.
- Visual Studio 2010 and 2012 runtimes installed during Bit9 Server installation are not removed when you run the uninstall program.
- The Bit9 Database remains on the server system after an uninstall.

Chapter 3

Logging In to the Bit9 Console

This chapter explains how to log in to the Bit9 Console as an administrator. Logged in as an administrator, you can configure all aspects of the system and create hierarchical user accounts.

Sections

Topic	Page
Logging In to the Bit9 Console	62
Logging Out of the Bit9 Console	63
Changing the Administrator Password	63
Viewing User Activities in the Events Table	64
Using Help	64

Logging In to the Bit9 Console

The Bit9 Security Platform employs a browser-based user interface called the *Bit9 Console*. You can log in to the console from a supported web browser on any computer with network access to the Bit9 Server, including the Bit9 Server itself.

To use the Bit9 Console and online help, JavaScript must be enabled on your browser. In Internet Explorer, you may need to adjust your security settings or set the Bit9 Server address to be part of your Local Intranet or Trusted Sites zone in order to access the Bit9 Console. The security settings are accessed from the Internet Explorer **Tools > Internet Options** menu, on the **Security** tab.

For your initial login, you use the built-in administrator account `admin`.

To log in to the Bit9 Security Platform:

1. From any supported web browser, enter the fully qualified domain name or alias of the Bit9 Server (IP addresss may be used but a FQDN or alias is preferred):

`https://server_name`

If you installed a verifiable digital certificate from a third-party authority as part of Bit9 Server installation, you go directly to the Bit9 login screen (step 3).

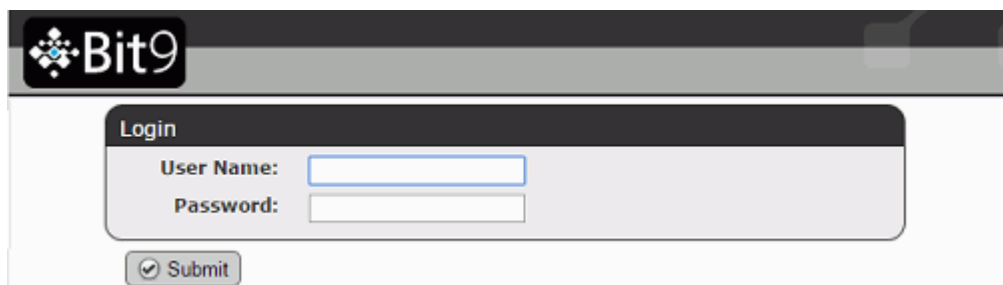
2. If you chose the Bit9 self-signed SSL certificate during Bit9 Server installation, the first time you enter the Bit9 Server URL, a certificate error appears. You can safely ignore the warning and click through the remaining confirmation screens. The warning appears because the authority of the self-signed certificate cannot be verified.

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**.

3. When the Bit9 login screen appears, enter the default user name (`admin`) and password (`admin`).



4. Click the **Submit** button. The Bit9 Console Home page appears.

You should change the password for the `admin` account after logging in. See [“Changing the Administrator Password”](#) on page 63.

Note

For environments that require best security practices, Bit9 recommends using AD-based login accounts. See the separate *Using the Bit9 Security Platform* guide for more information about AD-based logins.

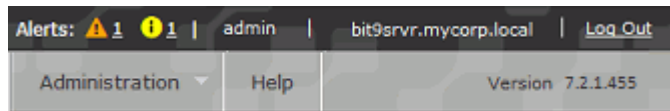
The console automatically logs users out after a specified period of inactivity. This can be modified on the System Administration page Advanced Options tab. You can modify the default starting page for the console using the dialog that appears when you choose **Tools > Preferences** on the console menu. See the online help in the console for additional information.

Logging Out of the Bit9 Console

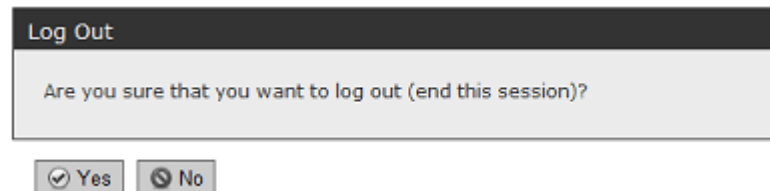
A logout link appears in the top right corner of the banner of the Bit9 Console web page. Logging out ends your session.

To log out of the Bit9 Console:

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



2. Respond to the confirmation prompt:



Changing the Administrator Password

For security, regularly change your administrator password. After logging in to the built-in administration account `admin` for the first time, you should immediately change the password, which initially also is `admin`.

To change the default administrator password:

1. On the Bit9 Console menu, choose **Administration > Login Accounts**.
2. On the Login Accounts page, click the Edit (pencil and file) button next to the `admin` user.

3. From the Edit Login Account, change the password as follows:
 - a. In the Password field, enter the new password.
 - b. In the Confirm Password field, enter the password again.
 - c. Click the **Save** button.

Note

A Bit9 administrator can use this same series of steps to change the passwords of other users if their accounts were created *in* the Bit9 Console. If a user logged in to Bit9 Console with an AD user account, that user's details, including password, cannot be modified in the console.

Viewing User Activities in the Events Table

You can review the combined event and exception logs in the Bit9 Console Events table. Messages include a record of user actions, including logins, new users created, and changes to user accounts.

To view Bit Server log entries:

1. On the Bit9 Console menu, choose **Reports > Events**. The Events page appears, and by default shows All Events in the past hour in the table at the bottom of the page.
2. If you want to see a subset of the available events, you can make a choice on the Saved Views menu or create a special view using Show/Hide Filters and Show/Hide Columns.
3. If you want to use a different time range, choose a time from the Max Age menu, or click the Show/Hide Filters link to configure and **Apply** a more complex time range. The report table at the bottom of the page updates to show the new time range.


The “Event Reports” topic in *Using the Bit9 Security Platform* or online help describes other event report types. The log of events, which grows over time, is automatically pruned by the Bit9 Server according to the schedule you set so it requires no manual maintenance. For more information, see the *Using the Bit9 Security Platform* guide or Help. To configure events to be output to a Syslog server from the Bit9 Console after installation, see the *Using the Bit9 Security Platform* guide or online Help.

Using Help

If you have questions about features outside of the installation and configuration tasks described in this manual, the Bit9 Console provides a context-sensitive Help system from which you can also navigate to other topics:

- When you click the **Help** button in the console menu, the *Using the Bit9 Security Platform* guide opens with an introductory screen and a table of contents.
- When you click a help button on an application page, the topic relevant to that page appears in addition to the table of contents.

To display online documentation from the Bit9 Console:

1. Launch **Help** either of the following ways:
 - From any application table, click the Help  button.
 - On the console menu, click **Help**.
2. From the contents frame, review the displayed help topic or select your topic of interest.
3. To view more topics, expand the contents tree.
4. To view an alphabetical listing of topics, click the **Index** button. Each index entry is hyperlinked to the associated topic.
5. To search key words, click the **Search** button, enter search terms, and click **Go** or press **Enter** on your keyboard.

Index

A

Active Directory
 integrating Bit9 Server with 16
 integrating Bit9 with 20

B

backup
 before server upgrade 52
 certificates 52
 re-enabling after upgrade 55
Bit9 agent
 and server upgrades 53
 diagnostics 34
 enabling management access 34
Bit9 Connector
 and Bit9 Server upgrades 54, 57
 licensing for 12
Bit9 Console
 changing administration password 63
 default password 62
 logging in 62
 logging out 63
Bit9 Detection
 changes in Bit9 7.2.0 56
 version in 7.2.0 upgrade 53
Bit9 Security Platform
 license keys for 12
Bit9 Server
 and Active Directory 20
 installing 22

installing and reconnecting/restoring a
 database 37
 license keys for 32
 network domain 15
 uninstalling 58

browsers
 JavaScript settings 17
 security settings 17, 62
 supported 17

C

certificates
 backing up before upgrade 52
 Bit9-supplied 62
console. See Bit9 Console

D

database
 restoring from backup 42
database size warning
 for upgrades 54
detection
 in Bit9 Server 7.2.0 53
documentation, Bit9 Security Platform 64

E

events log 17, 64
 integrating with Syslog 64

F

FAT file systems 15

file systems, supported 15

H

Help, online. See online Help

I

installation

- and reconnecting/restoring a database 37

- Bit9 Server 22

- overview summary 13

- Windows Server 15

Internet Information Services (IIS)

- as Bit9 web server 16

- configuration requirements 16

IP address

- active with multiple NICs 28, 45

- default 27, 45

- server 27, 45

J

JavaScript 17

L

license agreement, Bit9 23, 38

license keys 12, 32

- for optional features 12

log files 64

- for server installation 35

logging in 62

logging out 63

N

network domains 15

- Active Directory 20

network requirements 16

NTFS file systems 15

O

online Help

- displaying 64

- JavaScript requirements 17

P

Parity account for SQL access 14

Parity agent. See Bit9 agent

Parity Server. See Bit9 Server

password

- Bit9 admin account 63

- Bit9 admin default 62

- for SQL login 25, 40

privileges, Windows administrator 20, 58

R

rebooting server

- after uninstalling Bit9 Server 58

reformatting, server disk 15

requirements

- browser 17

- installation privileges 20

- network 16

- server IP address 27, 45

- supported browsers 17

- uninstallation privileges 58

S

server upgrades 50

SQL Server configuration

- for Parity access 14

Syslog output 64

U

uninstalling Bit9 Server 58

upgrading

- blocked access warning 53

- database size requirements 54

- with agent on server computer 53

upgrading Bit9 Security Platform

- agent upgrades 56

upgrading Bit9 Server 50

users, Bit9 Console

- changing password 63

- default password 62

- login 62

utilities, server management 15

V

Visibility

- licenses for 12

W

web servers

- automatic startup 16

supported 16
Windows Server
bundled management utilities 15