
# Bit9 Security Platform 7.2.1

# Release Notes

**Product Version 7.2.1.2102**
**Patch 14**
**13 May 2016**

**Carbon Black, Inc.**
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: http://www.carbonblack.com

# Introduction

The *Bit9 Security Platform v7.2.1 Release Notes* document provides information for users upgrading from previous versions as well as users new to Bit9 Platform. It consists of the following major sections:

**Before you begin**: This section describes preparations you should make before beginning the installation process for Bit9 Server.
**Bit9 Platform 7.2.1 new and modified features**: This section provides a quick reference to changes in the Bit9 Platform made since Bit9 Platform 7.2.0.
**Corrective content:** This section describes issues resolved by this release as well as more general improvements in performance or behavior.
**Known issues and limitations:** This section describes known issues or anomalies in this release of Bit9 Platform v7.2.1 that you should be aware of.
**Contacting Bit9 support:** This section describes ways to contact Bit9 Technical Support and the information to have prepared to troubleshoot a problem.

This document is a supplement to the main Bit9 Platform documentation.

## About your Bit9 Platform Distribution

Your Bit9 Platform distribution includes the Bit9 Server installation program and documentation files. Bit9 Server custom-generates agent installation packages at your site for each protection policy you define, so no separate agent installer is needed in the original distribution.

## Purpose of This Release

This release contains corrective content that resolves reported issues. Please review the "Corrective Content" and the "Known Issues and Limitations" sections carefully.

This release also will enable VirusTotal hash lookups by default for new installations.

## Documentation

Your Bit9 Platform documentation set consists of online Help built into the Bit9 Console and additional documents in PDF format available on the Bit9 Support Portal. The standard documents include:

**Installing the Bit9 Server:** Provides instructions for installing and configuring the Bit9 Server.
**Using the Bit9 Security Platform:** Describes Bit9 Platform operation, including step-by-step instructions for administration and configuration tasks. Management topics for computer systems, including agent installation, are also covered.
**Bit9 Platform Events Integration Guide** – Describes the events that are generated, tracked, stored, and accessible through the Bit9 Platform system, and the ways you can access Bit9 Platform event data outside of the Bit9 Console user interface.
**Bit9 API Documentation** – Instructions for configuring the Bit9 API are included in *Using the Bit9 Security Platform.* Up-to-date documentation of the actual API objects and properties, as well as code examples, is available at: https://github.com/carbonblack/bit9platform

# Before you Begin

This section describes preparations you should make before beginning the installation process for Bit9 Server. These include actions you should take before installing Bit9 Server, preparations you should make for configuring the server after installation, and general information you should know about server and agent. It contains information that applies to upgrades and new installations.

## System requirements

The document *Bit9 Security Platform Version 7.2.1 Operating Environment Requirements* describes the hardware and software platform requirements for the Bit9 Server and the SQL Server database that stores Bit9 data. The document *Bit9 Agent Supported Operating Systems v7.2.1* provides the current requirements for systems running the agent. Both are available to customers with login credentials on the Bit9 Support Portal.

***Both upgrade and new customers should be sure to meet the requirements before proceeding.***

### *Additional downloads*

This section contains links to download additional software that may be required to install Bit9 Platform version v7.2.1. Consult the *Installing the Bit9 Server* guide for more information.

**Windows Installer 4.5:**
http://www.microsoft.com/en-us/download/details.aspx?id=8483

**SQL Server 2012 Express:**
http://www.microsoft.com/en-us/download/details.aspx?id=43351

## Bit9 Server Upgrades

Bit9 Server upgrades are supported from the following Bit9 Server versions to this 7.2.1 patch version:

- V6.0.2.449 Patch 17
- All 7.0.0 GA and Hotfix versions
- All 7.0.1 GA and Hotfix versions
- All 7.2.0 GA and Hotfix versions

For more detailed instructions, please refer to *Installing the Bit9 Server*. It is available on the Bit9 Support Portal.

This section is for upgrades only. If you are not upgrading, see New Bit9 Platform Installations (page 5).

### *Support for the upgrade process*

Bit9 Server and Agent upgrade support is covered under the Customer Bit9 Platform Maintenance Agreement. Bit9 recommends contacting Technical Support prior to performing the upgrade for further details on the upgrade process and the latest information that supplements the information contained in this document.

## *Rescanning of agents after server upgrade*

When Bit9 Server is upgraded from one major version to another (such as v7.0.0 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 also require a new inventory of files in any trusted directories to determine whether there are previously ignored files that are now considered interesting. This process involves the same activity as agent initialization, and can cause considerable input/output activity, which can require between minutes and many hours, depending upon the number of agents and the number of files. Bit9 recommends a gradual upgrade of agents to avoid an unacceptable impact on network and server performance. See "Enabling Automatic Agent Upgrades" in the *Using the Bit9 Security Platform* guide for more details.

## *Before running the server upgrade*

The following tasks should be done *before* you run the Bit9 Server upgrade program.

**Backup Bit9 Server database:** Backup your Bit9 Server database before you begin the upgrade process. You *must* have a recent backup available so that there is a recovery option in case of database update failure during server update.

**Backup certificates separately:** In v7.2.1, Bit9 Server's Certificates will be backed up in the Database. However, IIS certificates are not backed up automatically. Please do a separate backup of IIS certificates, and if upgrading from 6.0.2, all Bit9 Platform certificates, on a system other than Bit9 Server.

**Disable distribution systems:** If you use third party deployment mechanisms (e.g. SCCM), either: disable the distribution of the Bit9 Agent using SCCM, and use Bit9 Server for upgrading agents; or disable Bit9 Server from upgrading agents, and use your third party deployment mechanism to upgrade the agents.

**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 on database maintenance and backups activity. Stop any of these jobs, and confirm that no one else is using database before initiating the Bit9 Server upgrade.

## *Prepare for post-upgrade tasks*

You should be prepared to do the following tasks after you run the Bit9 Server upgrade program.

**Review external event settings:** If you use External Events, review the settings to ensure they are still enabled and correctly functioning. Also, the external event schema has been changed. Review the upgrade section of *Installing the Bit9 Server* for information on how to upgrade it.

**Review updaters:** New Updaters have been added. Review the Updaters tab on the Software Rules page to make sure the correct updaters are enabled. Note in particular these updater changes:

- In Parity 6.0.2, there were separate updaters for Java Virtual Machine only and for Java and Bundled Software. In Bit9 Platform v7.0.1 and later, there is a single updater called **Java** that replaces both of these, and when enabled, allows updates to Java and related bundled software.
- In Bit9 Platform v7.2.1, the native updaters for Mac and Linux, which were previously always enabled and unlisted, are now listed on the Updaters page and can be enabled and disabled.

- The SMS Software Approval updater has been removed because Microsoft SMS has reached its end of life. The replacement product is Microsoft SCCM, for which there is an updater in Bit9 Platform.

**Update agent distribution points:** If you use third party deployment mechanisms (e.g. SCCM), re-enable or re-create them using new agent packages from the upgraded Bit9 Server. Use ParityHostAgent.msi to upgrade from a pre-v7.0 agent.
**Review the new Bit9 Platform installations section:** Although it is for new installations, this section also includes information of possible interest to upgrade customers.
**Enable System Health indicators:** Bit9 Platform v7.2.0 includes a new System Health page, which reports on factors that affect the performance of your server, including the compliance of your environment with Operating Environment Requirements. Consider enabling this feature to keep your system health.

## New Bit9 Platform installations

For more detailed instructions about preparations you must make, please refer to *Installing the Bit9 Server*.

This section describes preparatory tasks and suggested post-installation tasks for new Bit9 Server installations. Although targeted at new installations, it should be reviewed by new and upgrade customers.

### *Prepare for Bit9 Server installation*

**Choose account for Bit9 Server installation**: Bit9 recommends that you use a Domain Service Account for Bit9 Server installation. If you plan to use Active Directory services or use an authenticated proxy to access the Internet, a Domain Account is required for Bit9 Server Service. This account must have Local Administrator privileges on the Bit9 Server.
**Note:** Do not change the permissions level of the account with which you install Bit9 Platform after installation.
**Prepare to enable Bit9 Agent management access:** The Bit9 Agent Management screen in the new installation dialog allows you to designate a user or group, or a password usable by anyone, to perform certain agent management activities assisted by Bit9 Technical Support. Especially if you will have client computers that will never be connected to Bit9 Server, it is best to set up a client access option before generating and distributing agent installation packages. If you are unable to configure access during installation, you can do it later on the Management Configuration page in Bit9 Console. See *Using the Bit9 Security Platform* (or online help) for more details.

### *Prepare for post-installation tasks*

**Enable Bit9 Platform CLI management access:** If you did not enable Bit9 Agent Management access during installation, go to the General tab of the System Configuration page in Bit9 Console to enable it, preferably before deploying agents. See "Configuring Agent Management Privileges" in *Using the Bit9 Security Platform* (or online help) for more details.
**Confirm agent installation privileges:** The Bit9 Agent installer must be run by a user with the appropriate administrative rights. On Windows, this can be either by Local System or by a user account that has administrative rights and a loadable user profile. On OS X and Linux, the user must be able to run as root (sudo is one of the techniques that may be used).

**Consider agent rollout impact:** As soon as the Bit9 Agent is installed, it connects with the server and begins initializing files. Because initialization can involve an increased flow of data between the Bit9 Server and its new client, be sure your agent rollout plans take your network capacity and number of files into account — simultaneous agent installation on all the computers on a large network is not recommended. Deploying agents in disabled mode will avoid this situation.

**Review trusted updaters:** Review Trusted Updaters to ensure the correct ones are enabled for your environment before you begin large-scale Bit9 Agent deployment.

**Review root certificates for trusted publishers:** Trusted Publishers are validated by Windows. For proper validation to occur, the correct, up-to-date root certificates must be installed for these publishers. You should ensure that Microsoft root certificate updates are included in your Windows Updates. If you plan to use in-house certificates, ensure that your in-house root certificates are installed on each endpoint on which you will install Bit9 Agent.

**Test user-supplied certificates:** Bit9 Server allows you to use user-supplied certificates for Bit9 Agent-Server communication. To validate this certificate, each agent system must have up-to-date root certificates. Bit9 recommends that you test your new certificates before large-scale Bit9 Agent deployment begins. See "Securing Agent-Server Communications" in *Using the Bit9 Security Platform* or online Help for more details.

**Review content of trusted directories for distribution systems:** If you use Windows Software Update Services (WSUS) or other software distribution mechanisms (e.g. SCCM or Altiris), pre-approving this content with a Trusted Directory before large-scale Bit9 Agent deployment will ensure a more effective transition to High Enforcement Level.

**Script Files:** It is most efficient to define your script rules before you enable to avoid having to rescan the file system to look for those scripts**.** Java Tracking is an example. Support for tracking Java class and jar files is not enabled by default. If you plan to track Java applications, please choose **Rules->Software Rules** from the console menu and enable the rules for Java on the **Scripts** tab.

**Exclude Bit9 Agent from AV scanning:** Antivirus products, including Microsoft SCEP, should be configured to exclude Bit9 Agent files from scanning. Please refer to the *Using the Bit9 Security Platform* guide for detailed information about the files or folders to exclude for each platform.

**Consider other agent interactions:** Certain other types of software may interact with the Bit9 Agent – contact Bit9 Support for more information on each of these cases:

- Disk encryption software may interact with the Bit9 Agent. In general, full disk or partition encryption should minimize the chances of problems. However, some encryption products are compatible with Bit9 Platform with other types of encryption (file or folder) enabled.
- Ghosting or imaging systems with Bit9 Platform pre-installed requires additional steps on the master system. Please consult the "Managing Virtual Machines" chapter in the *Using the Bit9 Security Platform* guide for more information.

**SQL recovery model:** The simple recovery model is recommended. Use of the full recovery model may affect Bit9 Server performance. If you intend to use the full recovery model, please contact Bit9 Support for more information.

**Enable System Health indicators:** Bit9 Platform v7.2.0 includes a new System Health page, which reports on factors that affect the performance of your server, including the compliance of your environment with Operating Environment Requirements. Consider enabling this feature to keep your system health.

# Bit9 Platform v7.2.1: New and modified features

The following sections provide a quick reference to the feature changes made since v7.2.0. These features are documented in *Using the Bit9 Security Platform* and the online Help in the Bit9 Console.

## VirusTotal hash lookups enabled

As of this release, we enable VirusTotal hash lookups by default for new customers, or new deployments for existing customers. What this means for you (if you're a new customer or create a new deployment) is that new hashes that are discovered in your environment (but not the files themselves) are sent to VirusTotal for reputation lookup.

This change does not affect the opt-in status of existing Cb Enterprise Protection installations.

The benefit of enabling this is that Cb Threat Intel will request VirusTotal results for a hash, and if VirusTotal has seen the hash before, Cb Threat Intel will use the results as one piece of information to establish or change threat scores provided by Cb Threat Intel. This can help you to drive your security policy based on threat from Cb Threat Intel Reputation.

If you are an existing customer and have not enabled this feature, you can do so by going to System Configuration within the Console, clicking the Licensing tab, and clicking Options within the Bit9 Software Reputation Service Activation section. This will open a page where you can check "Enable VirusTotal lookup."

Likewise, if you are a new customer, or an existing customer establishing a new deployment, and would like to disable this feature, simply go to the page described above and uncheck "Enable VirusTotal lookup."

Note: If an existing server is given a new SID, that server will appear as a new customer and VirusTotal hash lookups will be enabled.

## Apple Mac OS 10.11.4 Agent Support

Beginning with v7.2.1 Patch 12, Bit9 agents are now supported on endpoints running on the Mac OS 10.11.4 version.

## Windows 10 Agent Support

Beginning with v7.2.1 Patch 6, Bit9 agents are now supported on endpoints running on the Windows 10 operating system.

## Export / Import of Bit9 Custom, Memory and Registry Rules

Custom, memory and registry rules can now be exported to an encrypted file and then imported into other systems, eliminating the need to manually recreate them. This simplifies the process of taking custom rules created in a test environment and moving them to a production environment, and allows Bit9 Support to more efficiently deliver solutions and new rules to Bit9 customers.

## Microsoft System Center Endpoint Protection Integration (SCEP)

Bit9 Security Platform v7.2.1 provides out-of-the-box integration with Microsoft SCEP. Some of the features of Bit9-SCEP integration include:

- Correlating SCEP-identified malware with Bit9 data allows you to determine:
  - Where malware exists/existed
  - Dwell time
  - Where it came in
  - Parent process that initiated it
- You can ban newly arrived malware using Bit9 after detection by SCEP.
- If the same parent process is identified as a repeated malware dropper, you can use Bit9 to ban the malware dropper rather than having to identify each piece of dropped malware and ban it separately.
- When SCEP is outdated or disabled, you can move Bit9 endpoints to High Enforcement policy for extra protection.

## REST API

A new Bit9 API is available for programmers who want to write code to interact with Bit9 Platform, either using custom scripts or from other applications. It is a RESTful API that can be consumed over HTTPS protocol using any language that can create get URI requests and post/put JSON requests as well as interpret JSON responses. Various Bit9 objects and properties are accessible for either read-only or read-write access through this interface.

## File Inventory Filtering

In v7.2.1, the Bit9 Platform includes an option to exclude from the Files on Computers inventory instances of supporting files signed by certain Microsoft publishers and approved in your Bit9 environment. Excluded files include DLLs and other supporting files, not actual applications.

Ongoing development in Microsoft Windows operating systems and Office releases has led to a very significant increase in the number of files they include, as well as in the files delivered when they are updated. This new feature may help reduce the need for new hardware to accommodate the increase in file inventory on Bit9 systems. It also can improve the performance of the Bit9 Server. The following list shows highlights of this feature:

- If this option is chosen, files identifying their publisher as "Microsoft Windows" or "Microsoft Corporation" will not have their instances added to the Files on Computers inventory if they are locally approved and match the definition of support files.
- Agents will still track all excluded files and send them to server. The only change this option invokes is eliminating these files from the Bit9 File Inventory (i.e., file instances).
- All associated events for excluded files will continue to be generated.
- Even with exclusion active, the Files on Computers inventory still includes files from these publishers if they are .EXE files (such as excel.exe, cmd.exe, powershell.exe, and calc.exe), and if they are in either the Unapproved or Banned state.
- Files from other Microsoft publishers are not affected by this feature.
- File Catalog entries are still tracked for these items, although their prevalence will be reported as zero since instances are not tracked.

- You can use Report Bans or Meters for excluded hashes (which are available in the File Catalog) to track instances of files that would otherwise be excluded.
- Exports to Analytics (Splunk) still contain historical data on instances of all excluded files.

## Bit9 Console User Interface Enhancements

The Bit9 Console user interface has had several improvements:

- **Adjustable Width Columns** – You can now change the width of columns in tables exceeding a certain width and not fitting in the current browser window. This feature is controlled on the Preferences page for each user.
- **Object Previews** – Certain console objects, including files and computers, now have popup object previews that provide additional summary information about highlighted items when you hover the mouse over them.
- **Improved Saved View Management** – You now have the option of clicking a Discard button to roll back changes you have made to a Saved View and return it to its previous saved state.
- **Event Search Capabilities** – You can now search for events by entering a string in a search box on the Events page. Entering the string pre-populates a filter to search for the string in key fields within the table.
- **File Search Enhancements** – On pages showing files, you can now select files and use the Action menu to search for computers with one or all selected files, or computers missing one or all of the selected files. Similar capabilities for one file are available on the Related Views menu for File Details and Instance Details pages.
- **Alert Priority Enhancements** – Alerts now have "priority" levels of High, Medium and Low, and may be filtered and grouped based on those priorities. In addition, wherever Alerts appear, the priority is shown using color-coded rows and/or icons to make identification of the most critical alerts easier.
- **Alert History and Instance Pages** – The Alert History and Instances pages have been reorganized into a two-tabbed page to simplify the navigation needed to view details of a triggered alert.
- **Additional Hash Support in Alerts and Meters** – In this release, you may use SHA-256 hashes in your specifications for Alerts and Meters.

## System Health Indicators

A new System Health page provides Bit9 administrators with the ability to monitor factors that affect the performance of the Bit9 Server. It displays the output of Health Indicators that can warn you about problems on the Bit9 Server, the SQL Server, or the environment as a whole.

For example, your servers might not be in compliance with the Bit9 Operating Environment Requirements guidelines for the number of rules or endpoints being managed. Other changes in your hardware environment, such as a change in disk capacity or RAM, might negatively impact performance. The System Health page can help you see these trends before they become serious problems.

## Agent Health Data

Bit9 v7.2.1 includes additional agent health checks, which provide granular information regarding the health of each agent computer. An administrator can see the health status and all recent health check events for each agent.

## WildFire Private Cloud Support

This release supports integration of the Bit9 Platform with a locally installed WildFire private cloud device. This provides a WildFire option for sites that cannot or choose not to allow connection to a public cloud service, and also eliminates limits on the number of queries you can submit in any given time period. You can integrate multiple local WildFire appliances with a Bit9 Server, and analysis requests will be distributed among them.

# Corrective Content

## Corrective Content in Bit9 Platform 7.2.1 Patch 14 (Build 2102)

- Bit9 Reporter might lose SRS connectivity after Apr 2016 due to cert expiring [48523]
  Details: Cb Enterprise Protection uses a certificate to communicate with the Software Reputation Service to obtain file reputation, threat indicators, and Updaters. This certificate expired on April 21, 2016. A new certificate is included as part of this release.
  Applies to: Server

- Failure installing on databases with case sensitive collation [47710]
  Details: Installing the product on a database that is configured to have case sensitive collation causes " Critical Database Script 'create' failed" error. The installer no longer fail with this configuration.
  Applies to: Installer

- ID column not being displayed in the files on computer area [48463]
  Details: The ID column was hidden in the files on computer area. In this release the column now appears.
  Applies to: Server

- Cb Enterprise files are not being analyzed by FireEye [48426]
  Details: Cb Protection was unable failed to process files to pass to FireEye for analysis. The issue has been addressed in this release.
  Applies to: Server

- Wildfire File Analysis test not working for CbEP integration [48348]
  Details: A button that isused to test Palo Alto Networks connectivity to WildFire cloud did not work, the issue has been addressed in this release.
  Applies to: Server

- Change Local State displays without appropriate permissions [49078]
  Details: The Console previously displayed the Change Local File state option in the right hand menu of the Computer Details page, without requiring the Computers Change advanced options permission be set. Change local file state will fail without that permission. This change prevents the option from being displayed unless the permission is set.
  Applies to: Server

- Max Agent Version can not be set to 0 in Updaters during upgrade. [48937]
  Details: A defect in the updater logic prevented the updated rule from being pushed to more recent agents. We have modified the current version when rule was modified from the Console.
  Applies to: Server

- The database is generating a SQL Exception [46431]
  Details: After upgrading from 7.2.1 Patch 3 to 7.2.1 Patch 6, a Database task SQL exception is thrown: ProcessEventRules - Arithmetic overflow error converting expression to data type int. The process event rules has been fixed to handle the maximum number of event ids.
  Applies to: Server

- Google Chrome updater is being blocked on software reporter tool [48652]
  Details: The Google Chrome updater has been modified and released to address this issue.
  Applies to: Server

- Powershell script rule does not include powershell.exe process [48900]
  Details: Powershell script rule did not include the powershell.exe process, it just includes the fileassociation for ps1 and psm1. Poweshell.exe process has been added in this release.
  Applies to: Agent [All]

- Running 7.2.1 Patch 6 on a Domain Controller with low resources could cause crash of the system [49066]
  Details: In rare cases, when a system runs low on resources and experiences memory allocations failures, parity.sys driver may be attempting to dereference null pointer that results in system crash. The issue has been corrected in this release.
  Applies to: Agent [Windows]

- Some files are missing in the console for some machiens after enabling (from disabled state). [48834]
  Details: In certain scenarios, when moving hosts from disabled to enabled, the server was missing some files for certain hosts.
  Applies to: Server and Agent [Windows]

- Some files might block after a Windows Update on machines running Windows 8, 10, and Server2012 [48491]
  Details: Some system files could block after a windows update on machines running Windows 8, Windows 10, or Windows Server 2012.
  The "Windows 8,10, and Server 2012 Updates" updater was improved in order to avoid those blocks.
  Applies to: Server

- New files not immediately detected on very busy systems [48449]
  Details: A messaging limit may have caused some new files to be missed when a large number of new files is produced very quickly. The message limit is now removed.
  Applies to: Agent [Windows]

- Windows 2003 Server will not boot if there are other security products on the system [48535]
  Details: On a Windows 2003 server if other file system filters installed, such as security products or backup software, a deadlock may occur during system boot. This has been fixed in this release.
  Applies to: Agent [Windows]

- 'Failure to connect to daemon' error after attempted agent upgrade to 7.2.1 Patch 10 or later [49250]
  Details: Under rare conditions, it is possible for the daemon to hang when disconnecting from the kernel extension. If this happens, setting the agent configuration proprerty of osx_skip_kext_teardown=1 will circumvent the issue.
  Applies to: Agent [Mac]

## Corrective Content in Bit9 Platform 7.2.1 Patch 13 (Build 2002)

- System crash on Windows 2003 server when unloading Bit9 driver while 3rd party antivirus application is present [48142]
  Details: A compatibility problem with McAfee Virus Scan Enterprise was discovered due to an interaction in how the parity.sys driver and the McAfee mfehidk.sys driver implement registry filtering on Windows XP and Windows Server 2003. The problem would result in a BSOD if the parity.sys driver were unloaded, such as during an agent upgrade while the system was running The parity.sys driver has been modified to fix the incompatibility and avoid a BSOD. However to upgrade to this fixed version without risking a BSOD the older parity.sys driver must be removed prior to starting the upgrade.
  A potential procedure would be (but should not occur in conjuction with other software updates such as Windows Updates):
  1) Disable tamper protection on an system running and agent to be upgraded.
  2) Within the registry modify the 'start' value under HKLM\System\CurrentControlSet\Services\ParityDriver to have a value of '4'.
  3) Reboot the system. The agent will not be functional at this point in time, the agent upgrade should occur as soon as possilble to avoid unapproved files due to missed writes.
  4) Perform the agent upgrade as normal.Applies to: Agent [Mac]
  Applies to: Agent [Windows]

- Upgrade agent to accept new company name [47478]
  Details: Modified the agent installers to recognize the new company name on future upgrades (Carbon Black)
  Applies to: Agent [All]

- System crash when a very long path with a large number of elements (\) is included [47821]
  Details: Bit9 agent could crash the operating system during a very long path normalization. The path needs to have roughly 70 or more seperators ("\" backslash) included in it.
  Applies to: Agent [Windows]

- Single core systems with Bit9 installed are utilizing 100% of CPU of a system [47906]
  Details: Systems with single core has a periodic task in the kernel, which is scheduled every 15 minutes consumes 100% of the CPU core for several seconds, causing the system to be unresponsive. Changes are made to spread out the processing as to not impact the system.
  Applies to: Agent [Windows]

- Address a Kernel Panic on Mac [48168]
  Details: 7.2.1 Patch 12 only might cause Mac OS X which has been fixed in this release.
  Applies to: Agent [Mac]

- Microsoft Windows 10 automatic updater generating errors [48170]
  Details: Microsoft Windows 10 automatic updater no longer works. That issue has been addressed in this release, allowing Windows automatic updater to work properly.
  Applies to: Agent [48170]

- System crash when a very long path with a large number of elements (\) is included [47821]

Details: Bit9 agent could crash the operating system during a very long path normalization. The path needs to have roughly 70 or more seperators ("\" backslash) included in it.
Applies to: Agent [Windows]

- Policy filter for certain policies do not return results in the Files on Computers tab [47454]
  Details: Improvements have been made to the peformance of queires that report on file state.
  Applies to: Server

- The link to the Operating Equipment Requirement in the installer is incorrect [48482]
  Details: The link in the installer to the Original Equipment Requirement on the User eXchange community site was directing to 7.2.0 release instead of 7.2.1 release.
  Applies: Installer

## Corrective Content in Bit9 Platform 7.2.1 Patch 12 (Build 1903)

- Updated files unapproved after reboot [47561]
  Details: If an OS update required the computer to reboot after the update, the operating files would be unapproved when the computer restarted. Due to a change in OS X 10.10 we shutdown before we have a chance to finish our analysis backlog which causes us to label these files as unapproved. This issue has been fixed.
  Applies to: Agent [Mac]

## Corrective Content in Bit9 Platform 7.2.1 Patch 11 (Build 1825)

- CPU utilization that causes the POS application to close unexpectedly [46957, 42310, 44739]
  Details: Reduce periodic high CPU use by making image enumeration single threaded.
  Applies to: Agent [Windows]

- SQL server prerequisite check causes Bit9 Server upgrade to fail [47009]
  - Details: Recent updates to SQL Server changed the format of the SQL Server version number, which resulted in failure of the Bit9 Server installation during the SQL Server version pre-requisite check. In this release, the Bit9 installer will account for the cumulative updates of SQL Server and accommodate the format change.

  Applies to: Server Installer

- Events not being persisted in a timely fashion [47218]
  Details: Investigating a system with sizable memory consumption, it was observed that the events were not being persisted in a timely fashion. The change might have a slight performance impact, but safer, as it could cause loosing important events, and impact to the daemon.
  Applies to: Agent [Mac]

- Delayed or failed shutdown on Windows 10[46728]
  Details: During shutdown of Windows 10, the agent will fail, not allowing Windows to shutdown, the workaround was to logout and then shutdown.
  Applies to: Agent [Windows 10]

- System crash after application of a specific Microsoft patch[46762]
  Details: In rare situations, the system would crash after application of specific MS patches. This due to a service group order error which resulted in problems with service dependencies. This has been resolved in this release by changing the service group membership of the Bit9 Agent service..
  Applies to: Installer [Windows]

- Under low memory conditions, possibility of the Bit9 agent to crash [46938]
  Details: On rare occasions when a low memory condition occurs, the agent would not be able to handle low resources in the system causing it to crash.
  Applies to: Agent [Windows]

- When the same file is being modified concurrently by multiple threads, Bit9 could cause a deadlock[46940]
  Details: Bit9 agent could deadlock a system on extremely rare occasion when a file is being modified concurrently by multiple threads. This issue has been resolved.
  Applies to: Agent [Windows]

- Kernel exclusions don't help with slow network transfers [46959]
  - Details: When internal configuration properties were set to ignore all activity over the network, not all network access was actually ignored. This could result in slower network access or blocks on network files. The internal network exclusions now cover all network-based access.

  Applies to: Agent [Windows]

- Upgrading from v7.0.1 to v7.2.1 generates an error in the log [46963]
  Details: When upgrading from v7.0.1 to v7.2.1 “Arithmatic overfow error” is entered in the migrate.sql script.
  Applies to: Install

- The server patcher is backing up the wrong files [47082]
  Details: The installer patcher is backing up the wrong integration files, which will impact the reversal if installation fails.
  Applies to: Installer

- System process on Citrix VDI endpoint is continuously busy on 1 CPU [47083]
  - Details: An interoperability problem was found with Citrix VDI that could lead to the Bit9 Agent getting stuck and consuming a lot of CPU. This was caused by the Citrix product returning a non-standard error code when the Bit9 agent attempts to delete a registry key that doesn't exist. In this release, the Bit9 Agent works around this issue and will no longer get stuck trying to delete keys that don’t exist.

  Applies to: Agent [Windows]

- Missing logon information in console [47168]
  - Details: In Bit9 Platform v7.2.1 Patches 8-10, information about the last logged in user was missing from the logon SID. In this release, the SID information is correctly copied.
  - Applies to: Server

- Diagnostic files are not being deleted even if configured []
  Details: Selecting the option to delete the diagnostic files after upload was not working properly, and not deleting all diagnostic files. It now purges all the proper files.
  Applies to: Server

- Bit Agent crashes at service start [47176]
  - Details: Certain invalid certificate co-signer information for a file would cause the Bit9 Agent process parity.exe to crash. In this release, the agent checks if the co-signer valid and does not use the information if it is invalid.
  - Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 Patch 10 (Build 1752)

- Bit9 Agent crashing on Apple Mac OS 10.11.2 version [47057]
  Details: Apple recently released Mac OS 10.11.2 and we have identified an incompatibility with the Bit9 Agent which causes a system crash. This release addresses the incopatability.
  Applies to: Agent [Mac]

## Corrective Content in Bit9 Platform 7.2.1 Patch 9 (Build 1704)

- Bit9 Agent crashing on Microsoft Windows 2003 Server 64 bit edition [46999]
  Details: Address an issue with Microsoft Windows 2003 Server 64 bit edition that causes Bit9 Windows agent to crash.
  Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 Patch 8 (Build 1612)

- Updated files unapproved after reboot [39990]
  Details: If an OS update required the computer to reboot after the update, the operating files would be unapproved when the computer restarted. Due to a change in OS X 10.10 we shutdown before we have a chance to finish our analysis backlog which causes us to label these files as unapproved. This issue has been fixed.
  Applies to: Agent [Mac]
- Server fails to upgrade from 7.2.0 to 7.2.1 with error “Database cannot be accessed”[45664]
  Details: During a Server upgrade, if the optional server tamper protection was enabled, the Bit9 Server couldn’t access the database and upgrade failed. In this release, the upgrade program checks the status of tamper protection before attempting to connect to the database. If tamper protection is enabled, an error message is displayed and the user is instructed to disable server tamper protect during upgrade.
  Applies to: Server
- Outstanding file count in dascli status is inaccurate after resync [45862]
  Details: After an agent resync, the 'dascli status' command would report an incorrect count, often nearly 100%.
  Applies to: Agent [Windows]
- System performance slow due to creation of unnecessary file groups [45912]

Details: The agent was creating file groups when no new executable files were found, such as when an executable file was renamed. This led to unnecessary activity on the server. In this release, the agent will only create file groups when a new file hash is actually written.
Applies to: Agent [Windows]

- Mac Agents exhibiting poor performance with CPU usage spiking to 100% [46351]
  Details: Previous versions of the Bit9 Agent for Mac installed on OS X 10.9 and 10.10 exhibited CPU usage spiking to 100%, causing sluggish performance and impacting usablility. In this release, changes to default file rules prevent this problem from occurring.
  Applies to: Agent [Mac]
- Unable to enable/disable reputation approvals on policies [46362]
  Details: A rare issue resulted in a timeout when activating or deactivating reputation approvals for a policy. In this release, the database interface used by the Console to enable reputation approvals has been made more robust to prevent this issue.
  Applies to: Server
- Agent crash when collecting diagnostics [46477]
  Details: An agent with a zero-length database would crash when an attempt was made to upload its diagnostics to the server. This could occur if the database was corrupted. In this release, attempting to upload diagnostics from a zero-length database does not cause a crash.
  Applies to: Agent [Windows]
- Reporter log fills with "Error converting data type to nvarchar to datetime." errors [46494]
  Details: On a Bit9 Server running versions 7.2.0 Patch 12 or 7.2.1 Patch 4, the reporter log could fill up with multiple instances of the error "Error converting data type to nvarchar to datetime." In this release, changes to database configuration eliminate the cause of these errors.
  Applies to: Server
- SQL performance degradation causing console timeouts [46551]
  Details: The console frequently timed out when viewing file catalogue data and other pages, such as the System Configuration page. It was found that file exclusions were not operating properly. In this release, design changes in the encoding of file exclusion rules eliminates the problem.
  Applies to: Server
- Agent fails to connect to server after clean 7.2.1 install due to excesss login sessions [46557]
  Details: If a misconfigured agent machine caused a very large number of login attempts on the server, this could result in failure of the agent to connect to the server. In this release, the presence of a large number of login sessions from an agent does not prevent connectivity between that agent and the server.
  Applies to: Agent [Windows]
- Code cleanup: Remove exception handling around FltGetStreamContext() [46584]
  Details: In some cases, the Bit9 Agent would try to continue operating after an OS error, and would lose some debugging information in the process. This problem has been fixed.
  Applies to: Agent [Windows]
- A custom company logo is not appearing in the Notifier window on all agent machines [46656]

Details: If a user specified a custom notifier logo and the agent restarted before it was able to download the image, the agent would not make another attempt at the download after then restart. This caused the notifier to use the Bit9 default logo. In this release, the custom logo link is preserved across restarts, and once successfully downloaded, the custom logo appears in the notifier.
Applies to: Agent [Windows]

- Windows 10 agent machine hangs on shutdown. [46727]
  Details: With 7.2.1 Patch 6 installed, attempts to shut down a Windows 10 endpoint could result in the OS restarting after a delay while a black screen was displayed. In this release, There is a Windows 10 defect for which Bit9 has coded a workaround regarding service change notifications was implemented, and shutdown is successful.
  Applies to: Agent [Windows]
- Patch install fails to update Server [46799]
  Details: In previous releases, the SQL script for server patch installations was not creating a required table, and the upgrade would fail. In this release, the installation script creates this required table.
  Applies to: Server
- dascli password cannot be used to authenticate commands on a disabled agent [46860]
  Details: On an agent in disabled mode, dascli commands requiring a password would not authenticate and run when given the correct password. In this release, putting an agent into disabled mode does not prevent use of password-authenticated dascli commands.
  Applies to: Agent [Windows]
- Healthcheck: Unexpected number of Install Events [45623]
  Details: The agent was configured to use the install date to link install events. The install date changes on each patch or repair operation, which prevents the events from being correctly detected as part of the same install. In this release, that install date is no longer used to distinguish events.
  Applies to: Agent
- Cluster status of database not identified in installation log [45684]
  Details: Previously, the installation log for a new or upgrade server installation did not identify whether the database used for the server is a cluster or single server. In logs from this release forward, cluster status will be recorded for use in resolving installation problems.
  Applies to: Server
- Unapproved files on remote drive can execute when run from command line [46520]
  Details: On Windows XP SP3 systems, an agent in high enforcement occasionally allowed an unappoved file to be executed from a network share if done via a command prompt. In addition, the notifier would incorrectly indicate that the execution was blocked. Command prompt executions of unapproved files on XP SP3 are now blocked as expected.
  Applies to: Agent [Windows]
- Unable to filter Approval Requests on Submitted Status [46644]
  Details: On the Approvals Request page (Tools->Approval Requests), the Status filter showed check boxes only for the Open and Closed statuses. . In this release, the user can also filter for Submitted requests (i.e., requests not yet opened or closed).
  Applies to: Server
- Heavy process load causes Bit9 agent to crash [46265]
  Details: Due to a missing thread lock, an agent under heavy process load could crash. In this release, the lock has been added and crashes related to this condition have been eliminated.
  Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 Patch 7 (Build 1562)

- Events for blocked files are not being received by the server [46119]
  Details: When an agent state was restored to an earlier state, such as would happen if a virtual machine were restored to an earlier shapshot, new agent events sent to the server going forward were being identified by the server as duplicates. This occurred until the total number of events sent to the server by this restored agent matched the number of events recorded in the server prior to the agent restoration. In this release, the server recognizes that the agent has gone back in time and uniquely identifies new events recorded from that agent.
  Applies to: Agent, Server

- Agent goes offline and parity service needs to be restarted [46120]
  Details: When a Bit9 background database cleanup task ran on a large database, it could cause the agent to run out of memory, terminating the parity.exe process. In this release, the cleanup task was altered to avoid impacting agent memory.
  Applies to: Agent [Windows]

- Windows agent won't connect to a server configured to use TLS 1.2 [46121]
  Details: Secure winhttp protocol TLS 1.2 was not supported in previous versions of the Bit9 Agent, and so a server configured to use TLS 1.2 could not connect to agents. In this version of Bit9 Platform, TLS 1.2 protocol is supported. For information, call Bit9 Technical Support.
  Applies to: Agent [Windows]

- Servers crashed and needed power cycle to recover[46122]
  Details: Under heavy load, servers became unresponsive due to issues with memory locks. This required the hardware to be restarted. In this release, memory is locked and unlocked appropriately for the process that caused the crash.
  Applies to: Server

- Multiple crashes due to malformed .msi file [46123]
  Details: If a malformed MSI file contained blank filename entries in its install list, agents attempting to analyze the MSI caused their hosts to crash. In this release, this condition is safely handled without causing a crash.
  Applies to: Agent [Windows]

- Incorrect path separators reported for autostart files [46124]
  Details: In 7.2.1, Bit9 Platform provides the ability to examine the list of autostart files, and in some cases, the path separators shown were incorrect, such as "/" being shown ans "\". In this release, the path separators are correctly shown.
  Applies to: Agent [Windows]

- Server upgrade ends with error "Arithmetic overflow converting expression to data type int" [46125]
  Details: When a Bit9 Server with a very large data base was upgraded from 7.2.0 to 7.2.1, the upgrade could end with a non-critical arithmetic overflow error. In this release, the error does not occur.

Applies to: Server

- Endpoints in local approval get multiple approvals for the same files [46132]
  Details: Files that were overwritten with the same contents, copied or renamed could generate multiple approval events. In this release, only one approval event is generated per locally approved file.
  Applies to: Agent [Windows]

- Notifier does not show on Citrix VDI machines in notifier policy [46134]
  Details: Prior to this release, on Citrix VDI endpoints, unapproved files were successfully blocked but in some cases the notifier dialog was not being displayed. This occurred when the process attempting an action was not run by the logged-in user or the System process. In this release, the notification is displayed in these cases.
  Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 Patch 6 (Build 1128)

- None.

## Corrective Content in Bit9 Platform 7.2.1 Patch 5 (Build 1101)

- Downloads of interesting files can fail to complete, resulting in file blocks [45208] [45626]
  Details: A problem was identified whereby the agent could compute the hash of a file that was still being written to, which resulted in an incorrect hash and blocking of the file. In this release, this problem has been addressed.
  Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 Patch 4 (Build 798)

- Unable to connect to local Wildfire WF-500 appliance [44262]
  Details: When a Bit9 Server attempted to connect to a Wildfire WF-500 appliance through the Bit9 connector, the connection attempt failed with the error “Unable to connect to appliance: Wildfire not accessible”. In this release, the WF-500 appliance and Bit9 Server connect successfully with no error displayed.
  Applies to: Server

- HTTP 500 error when changing a custom rule’s rank more than approximately 100 positions [44291]
  Details: Using either Firefox or Chrome browsers, changing a custom rule’s rank more than approximately 100 positions caused an HTTP 500 timeout error. In this release, changing the rank of custom rules by many positions does not cause the browser to timeout.
  Applies to: Server

- Double dashes around policy names not displayed after using quick search on the Computers page [44307]

Details: When policy names are automatically assigned using Active Directory policy mapping, double dashes surround the policy name. These disappeared after Search box bar was used on the Computers page. In this release, the double dashes always surround the automatically assigned policy name.
Applies to: Server

## Corrective Content in Bit9 Platform 7.2.1 Patch 3 (Build 710)

- Random blocks on Windows system files after upgrading to 7.2.1 Patch 2 [44564]
  Details: Upgrades to 7.2.1 Patch 2 resulted in occurrences of random Windows system files being blocked. In most instances, the hashes displayed for these files were blank. In this release, the issue that caused the blocks of Windows system files has been eliminated.
  Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 Patch 2 (Build 705)

Console reports fatal network error after upgrade to 7.2.1 [44114]

- Details: After an upgrade from 7.2.0 to 7.2.1, the console reported "Fatal Error – Network error while trying to communicate with Bit9 Server". The console was then inaccessible and agents did not connect to the server. Performing uninstall/install resulted in the same error. In this release, , this error does not occur.
- Applies to: Server

## Corrective Content in Bit9 Platform 7.2.1 Patch 1 (Build 639)

System crash reported after upgrading to, or uninstalling from, certain builds of version 7.2.0. [41926]

- Details: A rare race condition could occurr during upgrade to, or uninstalling from, certain builds of 7.2.0. This was caused by premature loading of the Bit9 driver, before the Bit9 registry keys were present, and led to a system crash. In this release, changes to the installer prevent this race condition and the crash does not occur upon upgrade or uninstall.
- Applies to: Server

Bit9 points to wrong source for files on Carbon Black Watchlist [43309]
Details: Bit9 reported incorrect endpoint names for files reported on the CB watchlist. In this release, improvements to the management of deleted hosts have solved this problem.
Applies to: Server

Subject Alternate Name is not validated on Certificate server installer dialog [43635]

- Details: In previous releases, the SAN field entry on the certificate creation dialog was not being properly validated during server installation. In this release, the installation dialog prompts the user to correct improperly formatted SAN field entries.
- Applies to: Server

Windows API allows users running agents in High Enforcement to bypass execution blocks. [43926]

Details: With the Windows API, a user whose system had an agent in High Enforcement could activate the Bit9 notifier's "Allow" button, which is normally invisible at this enforcement level. This would permit the execution of any file. In this release, the "Allow" button cannot be activated on systems running in High Enforcement.

- Applies to: Agent [Windows]

## Corrective Content in Bit9 Platform 7.2.1 (Build 551)

Software Reputations Services proxy field allows only URL format. [38398]

- Details: In previous releases, the address provided to use a proxy for Bit9 SRS access had to be in URL format: *http://proxy server:port*. In this release, you can use this format or use an IP address or hostname without the "Http" prefix: *hostname_or_ip[:port]*
- Applies to: Server

When MD2RSA certificates are excluded, an error is displayed [40035]

- Details: If you attempted to exclude the use of MD2RSA certificates using the switch on the System Configuration page Advanced Options tab, an error "Error updating config prop" was displayed when trying to save the change. In this release, this error condition does not occur.
- Applies to: Server

Disabled computers appear as 100% initialized on the Computers page [40056]

- Details: On the console Computers page, if you grouped computers by "% Initialized", disabled agents appeared in the console as part of the group that was 100% initialized. In this release, disabled agents are now included in the 0% initialized group. Also, the agent details for those disabled agents will not show initialized per cent or synchronized per cent.
- Applies to: Server

Error when selecting Local Administrators, Local System or Service Accounts in the User field of a custom rule [40997]

- Details: An error occurred when a custom rule was created as follows:
  - When prompted for user or group, choose "Specific User or Group".
  - Enter any letter and wait for the dropdown list.
  - Select "Local Administrators", "Local System" or "Local Service".
  - Save.

  This error was displayed: "Error: SID for 'xxxx' was not found" (where xxxx is your selection in the example above).

  In this release, 'Local Administrator', 'Local System', and 'Service Accounts' will correctly map to the proper group and not show an error, whether typed in or chosen from a menu.

  **Note:** If you have created your own group that uses one of these names, entering it manually will resolve to your group, while selecting it in the dropdown will resolve to the System group.
- Applies to: Server

Trusted Publisher approvals not allowed if publisher name varies by case [41236]

- Details: Publishers whose names differed only in case were not being properly distinguished, and files from approved publishers with some of these case variations were not being approved. In this release, Bit9 server will now distinguish between file publisher names that differ only by case. Each variation by case of publisher name can be approved or banned independently.
- Applies to: Server

Error message when filtering by Computer Name on the Approval Requests page [41563]

- Details: On the Approval Requests page, filtering for 'Computer Name' using the options 'is', 'is not' and 'begins with', caused an error to be displayed: "Invalid field:Computer". In this release, the autocomplete feature for Computer Name on the Approval Requests page has been corrected to avoid this error.
- Applies to: Server

Selected encrypted USB drives cannot be accessed or approved [42213]

- Details: When McAfee and MXI Stealth M500 encrypted USB devices were remounted, they were treated as if they had been removed. All file operations were then blocked. In this release, remounting the device is no longer treated as device removal and file operations are not blocked.
- Applies to: Server

The Bit9 API Computer object returns the wrong value for “policyDescription” [43270]

- Details: In the new RESTful Bit9 API in pre-release versions of 7.2.1, the Computer object had an incorrect label “policyDescription” for the property that returns the computer description. This is now correctly labeled “description”.
- Applies to: Server

Imported custom rule has [1] appended to its name [43274]

- Details: In pre-release versions of v7.2.0, after exporting a custom rule, deleting the exported rule and then importing the custom rule, the imported custom rules had “[1]” appended to the rule name. In this release, the custom rule name is displayed correctly.
- Applies to: Server

CB Watchlist Hits point to wrong source in CB [43309]

- Details: When a Carbon Black server is integrated with the Bit9 Server, Carbon Black Watchlist events reported to the Bit9 Console sometimes pointed to the wrong Bit9 Agent. In this release, the error has been corrected.
- Applies to: Server

Server installer does not halt if it fails to stop services [43378]

- Details: During an upgrade attempt, in some cases the services included in the Bit9 Platform product were not stopped, resulting in a failed upgrade. In this release, the server will properly halt if a service cannot be stopped.
- Applies to: Server

# Known Issues and Limitations

On minor updates on the Mac OS 10.11 it is possible some system files will not get approved, causing the operating to slow [48578]

- There are two options as a workaround for this issue
  - Approve the unapproved files
  - Put the agent in locall approval mode or in low enforcement before upgrading

Bit9 Platform V7.2.1 installations failure due to changes in the latest Microsoft SQL Server updates: [47099]

- We have identified an issue with Bit9 7.2.1 installations that occurs due to changes in the latest SQL Server updates which changes the format of the SQL Server version number. The result is that the Bit9 install will fail the SQL Server version pre-requisite check.
- With the latest SQL Server updates applied, the Bit9 7.2.1 server install will fail when:
  - Upgrading from a pre-7.2.1 release
  - Installing a new Bit9 server
- Affected Microsoft SQL Server versions:
  - SQL Server 2012 SP2 CU8+
  - SQL Server 2014 SP1 CU3
- Note that patch installs are not impacted.
- What should you do?

  If you have not installed the upgrade to Microsoft SQL Server but would like to, please upgrade the Bit9 Platform first before upgrading SQL Server, then upgrade your SQL Server.

  If you already have upgraded your SQL Server there are two options:

- Wait for a patch to be released which will address the issue. A release plan will be available in a few days and will be communicated to you.
- Uninstall the Microsoft SQL Server cumulative upgrade, install or upgrade Bit9 Platform Server, then upgrade SQL Server.

The files FireEye.dll and Bit9.FireEye.dll should have version numbers that are unique to the Bit9 version and build in which they appear. However, both Bit9 7.2.1.705 and Bit9 7.2.0.705 report version number 1.0.2.705 for these files. [44286]

Starting in 7.2.1 Patch 2, the Linux agent package is not included in the installer. However, the 7.2.0 Linux agent is compatible with the 7.2.1 Bit9 server. To deploy the 7.2.0 Linux agent, you should download the Linux installer from the Bit9 + Carbon Black customer portal or the User eXchange, and follow instructions listed below:
From the latest 7.2.0 agent, copy these files

- b9agent.rpm
- b9notifier.rpm
- Bit9Redhat6Install.bsx

into the 7.2.1 server at folder c:\Program Files (x86)\Bit9\Parity Server\hostpkg.

In that directory in the server:

- Rename the file b9agent.rpm to b9agentRedhat6.rpm.
- Make a copy of the same file and rename the copy to b9agentRedhat7.rpm
- Rename the file b9notifier.rpm to b9notifierRedhat6.rpm.
- Make a copy of the same file and rename the copy to b9notifierRedhat7.rpm
- Make a copy of the Bit9Redhat6install.bsx file and rename the copy to Bit9Redhat7install.bsx
- In the server, navigate to: https://<myservername.mydomainname>/shepherd_config.php
- Set the property "GenerateRedhatInstaller" to "true"
- Restart the server.

The host packages displayed in the server will now include "Redhat". [44255]

- During 7.2.1 server install, a pop-message will occur if the indicated Microsoft packages are not already installed:
- Status: Requirement
  Pending: Microsoft Visual C++ 2010 SP1 Redistributable Package (x86)
  Pending: Microsoft Visual C++ 2012 SP1 Redistributable Package (x86)
- (options) Install / Cancel
- Since these two packages are required, the proper option to select is "Install".

The "Operating Environment Requirements" document has been updated to add these packages to the system requirements. [43766]

The Administrator Login Account group can be disabled, and if you have not created another group and account with full administrative privileges, you may not be able to access the Bit9 Console interface to re-enable it. To correct this, enter "ParityServer.exe /adminReset" from the command line. Note that this will also restore all admin permissions and the default admin/admin password. [40145]

After the server is upgraded from v6.0.2 to v7.2.1, the globally defined password for agent management does not work on the command line interface for new agents. For these upgrades, if you used a global password, it must be reset on the General tab of the System Configuration page. [38051]

Registry Rules that use a path containing links will not work. For example, if you use a path with *HKLM\SYSTEM\CurrentControlSet*, the rule will not work because CurrentControlSet is a link to the other ControlSet(s). To work around this limitation, consider using wildcards in the path to cover all of the cases to which you need to apply the rule; in the example above, you might use *HKLM\SYSTEM\ControlSet** . [37562]

An underscore at the end file name filters is ignored because an underscore in SQL is interpreted as wildcard character. [18103]

In rare cases, agent upgrades may be blocked because older Bit9 MSI or MSP packages referenced during upgrade have no global file state. This can occur after a server upgrade from a release *prior to* 6.0.2.228, 7.0.0.1229, or 7.0.1.1109. If you have upgraded from a version prior to those listed, you may have this problem if:

- Users report that the Bit9 Platform Notifier shows MSI or MSP blocks after you have enabled agent upgrades.
- On the console Events page, you notice multiple file block events for the same MSI or MSP files.
- Agents have an Upgrade Status of "Upgrade Scheduled" but do not ever change to "Up to Date" and have an Upgrade Error of "Agent Upgrade: Unknown error executing" or "Agent Upgrade: Failed executing".

If this situation occurs, do the following:

1. **Turn off automatic agent upgrades:** In the Bit9 Console, go to the **Administration > System Configuration** page and click on **Advanced Options**. On the Advanced Options tab click the Edit button at the bottom of the page, in the Bit9 Agent panel, choose Disabled on the menu, and then click the Update button at the bottom of the page.
2. **Locally or globally approve the Bit9 MSPs or MSIs that are blocking.**
3. **Turn automatic upgrades back on:** Follow the same procedure as step 1, except choose Enabled on the menu.

**Note:** If you are using a third-party software distribution method to upgrade agents, disable that distribution until you approve the blocking files.

If you encounter this situation and are unsure of whether to approve the blocked files, contact Bit9 Technical Support.

If you use the "Export to CSV File" feature in a Bit9 Platform table (such as the Computers page), there is a limit of 25,000 on the number of rows that can be exported.

Some or all memory rules are not supported on certain Windows based operating systems:

- Memory rules are not supported on Windows Server 2003 64-bit.
- Kernel Memory Access rules are supported only on computers running Windows XP or Windows Server 2003 without SP1.
- Dynamic Code Execution rules are supported only on computers running 32-bit operating systems. On Windows XP, if the system-wide DEP Policy is set to "AlwaysOff", dynamic code execution memory rules cannot be enforced, but Bit9 Platform will report as though they were enforced. If the policy is set to "OptIn" (the default) or "OptOut", then these rules will be enforced on systems running XP.

On Mac OS X, an interoperability issue exists with certain versions of Trend Micro's endpoint security products. You must be running Trend Micro's TMSM version 1.5 SP4 or higher. [26565]

On OS X and Linux platforms, you cannot disable or replace the Bit9 logo in Notifiers. If you disable the logo, you may observe computer management events indicating "Computer failed to receive Notifier Logo: Source[…/GenericLogo.gif]". These should be disregarded. [26502, 24017]

Symantec Endpoint Protection and Bit9 Platform exhibit a conflict on Mac OS X with regard to Software Update. Some Software Updates are intermittently blocked by Bit9 Platform as a result. If an update is blocked, it can be approved by the Bit9 Console and applied again. To avoid future blocks on other endpoints, each blocked update can be globally approved.

Software Updates blocked by the SEP/Bit9 Platform interaction produce two events in the Bit9 Platform Events log: a Discovery event with a file written by installd followed by an Execution block (unapproved) event with installd as the process that attempted the execution. [26825]

When a Custom Rule is used to block writes to a specific file or set of files, and the rule is tested with an editor that creates a backup of the original file, it may appear that the rule is not correctly functioning. This is due to the functionality of certain editors, which may use a rename operation to replace the original file with its backup when any modification is aborted by the user. [29917, 33147]

When upgrading Bit9 Platform 7.0.1 or later from earlier releases, it may be necessary to update certain Microsoft SQL components. In this case, a Microsoft dialog will appear during the upgrade process. Follow the dialogs to update the associated Microsoft SQL components. Bit9 Platform upgrade will continue when this step is complete. [29819, 29822]

On Linux systems, the *ext3* file system does not perform journal checksums, which can lead to file system corruption when the disk controller is using out-of-order write caching. In some circumstances, this can lead to corruption of the Bit9 agent database. In order to avoid this, the option "*barrier=1*" must be added to /etc/fstab for all *ext3* file systems.

If the Notifier Link field causes the launch of an application that is not DEP compatible, the application may not launch when the link is selected, even if the associated application is already running. This occurs because Bit9 processes require DEP to be enabled as a security measure. Please contact Bit9 Support for assistance in creating Custom Rules if you run into this issue. [26943, 26971]

Known interactions with the VMware vShield Endpoint driver (*vsepflt*) can cause systems to deadlock in the presence of other filter drivers, such as Bit9. The *vsepflt* driver may be loaded on a virtual machine, even when vShield is not in use. Permanently disabling or removing the *vsepflt* driver will address this issue. [33719, 34411]

Changing the major or minor version of any operating system after installing the agent is not supported, and doing so will produce health check failures and in some cases failure of the upgrade. If you need to upgrade your operating system or you see a health check failure that reports a mismatch between the agent and the build platform, contact Bit9 Technical Support for remediation recommendations. Service pack upgrades are fully supported and do not cause health check failures. [33646]

For Mac and Linux, the default uninstall behavior is now to remove all Bit9 agent data. Previous releases required an additional parameter ("-d") for this data to be removed. The same parameter now prevents data removal, if this is required. [28824]

On Mac, when *chroot* is used, the patterns for script processors may need to be changed to patterns that will be appropriately matched in the re-rooted environment. For example, in place of "/bin/bash", you may want to use "*/bin/bash". Contact Bit9 Support for additional assistance. [34305]

Carbon Black integration applies only to Bit9 Platform Windows agents. Integration with Carbon Black Mac and Linux sensors is not available in Bit9 v7.2.1 [39284]

# Contacting Bit9 Support

For your convenience, Bit9 Technical Support offers several channels for resolving support questions:

| Technical Support Contact Options |
|---|
| Web: www.bit9.com |
| E-mail: support@bit9.com |
| Phone: 877.248.9098 (877.**BIT9**.098) |
| Fax: 617.393.7499 |
| Hours: 8 a.m. to 8 p.m. EST |

## Reporting Problems

When you call or e-mail Bit9 technical support, please provide the following information to the support representative:

| Required Information | Description |
|---|---|
| **Contact** | Your name, company name, telephone number, and e-mail address |
| **Product version** | Product name (Bit9 Server, Bit9 Agent, or Bit9 Software Reputation Service) and version number |
| **Hardware configuration** | Hardware configuration of the Bit9 Server or computer (processor, memory, and RAM) |
| **Document version** | For documentation issues, specify the version of the manual you are using. The date and version of the document appear after the copyright section of each manual. |
| **Problem** | Action causing the problem, error message returned, and event log output (as appropriate) |
| **Problem severity** | Critical, serious, minor, or enhancement |