Parity Version 7.0.1

Release Notes

Parity v7.0.1.2612
Patch 21
30 April 2015

Bit9, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@bit9.com
Web: http://www.bit9.com

Introduction

The *Parity v7.0.1 Release Notes* document provides information for users upgrading from previous versions as well as users new to Parity. It consists of the following major sections:

- **Before you begin**: This section describes preparations you should make before beginning the installation process for Parity Server.
- **Parity v7.0.0 and v7.0.1: New and Modified Features:** This section describes major changes since v6.0.2 and should be read by all users.
- **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 Parity v7.0.0 and v7.0.1 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 Parity documentation.

About your Parity Distribution

Your Parity distribution includes the Parity Server installation program and documentation files. Parity Server generates custom 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

The patch includes quality improvements and a bypass fix as a corrective content. Please see the corrective content section below.

Documentation

Your Parity documentation set consists of online Help built into the Parity Console and PDF files included with the product distribution and also available in the support area of the Bit9 web site.

- **Installing Parity Server:** Provides instructions for installing and configuring the Parity Server.
- **Using Parity:** Describes Parity operation, including step-by-step instructions for administration and configuration tasks. Management topics for computer systems, including agent installation, are also covered. This is available as a PDF file and in online Help.
- **Parity Events: Integration Guide** – Describes the events that are generated, tracked, stored, and accessible through the Parity system, and the ways you can access Parity event data outside of the Parity Console user interface.

Before You Begin

This section describes preparations you should make before beginning the installation process for Parity Server. These include actions you should take before installing Parity 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 7.0.1 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 v7.0.1* provides the current requirements for systems running the agent. Both are available in the support area of the Bit9 web site.

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 Parity version v7.0.1. Consult the *Installing Parity Server* guide for more information.

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

SQL Server Permissions

In order to allow diagnosis of Bit9 server issues, certain permissions are required for the SQL Server account. Please see *Preparing for Parity Installation* in the *Installing Parity Server* guide for more detailed information on these requirements.

Parity Server Upgrades

For more detailed instructions, please refer to the *Installing Parity Server* guide. It is available in the support area of the Bit9 web site.

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

Support for the Upgrade Process

Parity Server and Agent upgrade support is covered under the Customer Parity 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. Technical Support is available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

Rescanning of Agents after Server Upgrade

When Parity Server is upgraded, ongoing enhancements to “interesting” file identification and certificate handling make it necessary to rescan the fixed drives on all Parity-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 excessive impact on network and server performance. See "Enabling Automatic Agent Upgrades" in the *Using Parity* guide for more details.

Before Running the Server Upgrade

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

- **Backup Parity Server database** – Backup your Parity Server database before you begin the upgrade process. Built-in backup is disabled during upgrade and must be re-enabled once you are sure the upgrade was successful.
- **Backup certificates separately** – In v7.0, Parity 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.x, all Parity certificates, on a system other than Parity Server.
- **Disable distribution systems** – If you use third party deployment mechanisms (e.g. SCCM), either:
    - disable the distribution of the Parity Agent using SCCM, and use Parity Server for upgrading agents;
    - or disable Parity Server from upgrading agents, and use your third party deployment mechanism to upgrade the agents.

Prepare for Post-Upgrade Tasks

You should be prepared to do the following tasks after you run the Parity 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 Parity 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 Parity 7.0.1, there is a single updater called **Java** that replaces both of these, and when enabled, allows updates to Java and related bundled software.
    - 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 Parity.
- **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 Parity Server. Use ParityHostAgent.msi to upgrade from a pre-v7.0 agent.
- **Review the new Parity installations section** – Although it is for new installations, this section also includes information of possible interest to upgrade customers.

New Parity Installations

For more detailed instructions, please refer to the *Installing Parity Server* guide. It is available in the support area of the Bit9 web site

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

Prepare for Parity server installation

- **Choose account for Parity server installation** – Bit9 recommends that you use a Domain Service Account for Parity 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 Parity Server Service. This account must be assigned Local Administrator privileges on the Parity Server.
  Note: Do not change the permissions level of the account with which you install Parity after installation.
- **Review .NET configuration** – If Microsoft .NET 4 is installed on your Parity Server system with Windows 2008 Server, ensure that the IIS DefaultAppPool is set to use ".NET Framework v2.0.50727" by default.
- **Prepare to enable Parity agent management access** – The Parity 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 Parity 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 Parity Console. See the *Using Parity* guide (or online help) for more details.

Prepare for Post-Installation Tasks

- **Enable Parity CLI management access** – If you did not enable Parity Agent Management access during installation, go to the General tab of the System Configuration page in Parity Console to enable it, preferably before deploying agents. See "Configuring Agent Management Privileges" in the *Using Parity* guide (or online help) for more details.
- **Confirm agent installation privileges** – The Parity 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, 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 Parity Agent is installed, it connects with the server and begins initializing files. Because initialization can involve an increased flow of data between the Parity 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.
- **Review trusted updaters** – Review Trusted Updaters to ensure the correct ones are enabled for your environment before you begin large-scale Parity 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 Parity Agent.

- **Test user-supplied certificates** – Parity Server allows you to use user-supplied certificates for Parity 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 Parity Agent deployment begins. See "Securing Agent-Server Communications" in the *Using Parity* guide 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 Parity Agent deployment will ensure a more effective transition to High Enforcement Level.
- **Java tracking** – 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 Parity agent from anti-virus scanning** – Anti-virus products should be configured to exclude agent files and folders from on-access or real time scanning. Please refer to the "Managing Computers" chapter in the *Using Parity* guide for detailed information about the files or folders to exclude for each platform.
- **Plan deployment of "ghosted" or virtually imaged agents** – Ghosting or imaging systems with Parity pre-installed requires additional steps on the master system. Please consult the "Managing Virtual Machines" chapter in the *Using Parity* guide for more information.
- **SQL recovery model** – The simple recovery model is recommended. Use of the full recovery model may affect Parity Server performance. If you intend to use the full recovery model, please contact Bit9 Support for more information.

Parity v7.0.0 and v7.0.1: New and Modified Features

The following section provides a quick reference to the feature changes made since v6.0.2.

Upgraded Console Look and Feel

Parity v7.0 has an updated color palette and has added additional features to improve the consistency and aesthetics.

Console Terminology

Parity v7.0 key terminology changed to make it clearer and more descriptive for users. These changes are:

Previous Term	The New Term
Seccon	Enforcement Level
Lockdown	High (Block Unapproved)
Block & Ask	Medium (Prompt Unapproved)
Monitor	Low (Monitor Unapproved)
Online	Connected
Offline	Disconnected
Pending	Unapproved (Files, Publishers, Devices)

Additional Agent-supported Platforms

Parity v7.0.1 extends many features of the Parity v7.0 release to Mac OS X, and to Red Hat platforms. In Patch 17, CentOS is no longer supported. Please review the *Operating Environment Requirements* document for specific version information.

Cloud-driven Approvals

To help manage the flow of blocked files, Parity v7.0 introduces cloud-driven file and publisher approvals. Files and publishers are compared against the Bit9 Global Software Registry to provide a trust level, and, at the administrator's discretion, a policy can be set to automatically approve files based on an administrator-specified trust level.

Role-based Access Control (RBAC)

In addition to the three predefined groups ("administrators", "power users" and "read-only"), Parity v7.0 provides the ability to create custom User Groups. Custom User Groups are created with distinct sets of view- and action-related permissions based on the user's role. Parity Console users can be mapped to the new groups based on their Active Directory security group.

Instance-based Device Control

More granular device control has been added that shows individual device information at the serial-number level on Device pages. Devices may also be searched by computer. Device bans and approvals can be created based on serial number patterns.

IPv6 Support

Parity v7.0 supports both IPv4 and IPv6. The server automatically detects the availability of each protocol.

Approval Request Workflow

In a High Enforcement Level environment, end users may need to run software that has not yet been approved. Parity v7.0 allows the end user to notify a Parity administrator of his or her reasons to have certain software approved, so that the administrator can more efficiently respond to a blocked application. This feature reduces the amount of time that IT spends determining which software needs to be approved.

Custom Script Support

Parity v7.0 includes pre-configured rules for identifying many common script types and their processors, and allows users to enable Parity management of those they want to use in their environment. Administrators can also define additional scripts by registering the processor and the file type for any script not pre-configured in Parity.

Remote Reboot Capability

In Parity v7.0 an administrator can now complete a forced reboot of a computer from the console.

Enforcement Ability during Initialization

In Parity v7.0, policies are enforced during the initialization period.

250,000 Agent Computers per Server

The Parity Server has been optimized to handle up to 250,000 connections in Parity v7.0.

Enhanced VDI Handling

Parity v7.0 provides easy provisioning of virtual machines with the Parity Agent installed, faster deployment of cloned images to a large number of users with optimized initialization, and quick retirement of images once they are reverted to a snapshot or deleted from the VM infrastructure.

Enhanced Agent Health Checks

Parity v7.0 includes an agent health check which provides 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.

Control of Certificate Restrictions

In Parity v7.0.1, certificates used for approval of a file by publisher may be required to meet two specifications, which are configurable beginning in Patch 8:

- **Certificate Algorithm** – Certificates using any of the following algorithms may be allowed or excluded from use in publisher approvals: MD2RSA, MD5RSA, SHA1RSA, SHA256RSA.
- **Minimum Key Length** – Choices range from 512 to 4096.

For new installations starting with Patch 8, the default certificate values are a minimum key length of 1024 and exclusion of the MD2RSA algorithm from use in approvals. For installations that are upgraded to Patch 8 or later from either prior patches of 7.0.1 or from earlier versions, the default minimum key length is 512 and no algorithms (of the 4 listed) are excluded. These settings may be modified on the Advanced Options tab of the System Configuration page.

Beginning in Patch 9, several additional certificate-handling options appear on the Advanced Options tab of the System Configuration page.

- **Digital Countersignature** – This checkbox on the Advanced tab of the System Configuration page in the console determines whether a digital signature must be countersigned in order for Bit9 to approve the signed file by publisher. By default, the box is not checked (i.e., no countersignature is required). If the box is checked, signatures without countersigning certificates are not considered valid for use in approval by publisher.

  Note the following additional details of countersignature handling:
  - If the box is unchecked, signatures lacking a countersigner are only valid for the life of the signing certificate.
  - Regardless of this setting, if a countersignature is present, it must be valid for the digital signature to be considered valid.
- **Revocation Checks** – There are two new settings that control whether and how the agent does a revocation check for certificates:
  - **Initial Revocation Check** – This determines whether, and if so, how a certificate revocation check is done when a file is initially discovered on an agent.
  - **Background Revocation Check** – This determines whether, and if so, how a certificate revocation check is done in the background every 24 hours.

  For each of the Revocation settings, there are three possible values:
  - **Network** – If revocation information is not locally available then use the network to retrieve a certificates revocation status.
  - **Cache** – Use locally available revocation status information when performing certificate revocation (the network will not be used).
  - **None** – Do not perform certificate revocation checking.

Consider your agent deployment scenario when setting these values since they can have an impact on agent performance. For example, if you have offline agents, you might want to avoid using the Network option, especially for the Initial Revocation Check. Also keep in mind that the daily revocation check is performed in the background, and is less likely to have a negative impact on agent performance, whereas the initial revocation check setting may have a noticeable effect on agent performance.

Bit9 Connector Support for WildFire 6.0

Beginning with v7.0.1 Patch 10, the Bit9 Connector supports integration with WildFire 6.0 in addition to the previously supported versions. Installing one of these Parity Server patch releases is the only action required to add this support.

This latest version of WildFire introduces the following new features:

- Support for analysis of more file types
- Reporting of detonation results from more than one detonation environment (typically Windows XP and Windows 7) or static analyzer

Note: WildFire's XML reports may now be significantly larger than those in previous versions. Consider this when allocating storage for the active set of notifications sent to the Parity Server.

To support the new WildFire version, changes were made on certain Parity Console pages. Full documentation of these changes has been integrated into the console Help and Using Parity PDF version for the affected patch versions. They are summarized below:

- **Reporting Analysis Environment in Notifications** – In the External Notifications view, a new **Analysis Environment** column is available (and standard in the *Palo Alto Networks Notifications* Saved View) to indicate the detonation or analysis environment used to produce a WildFire 6.0 notification. Analysis Environment (if any) is also reported on the main External Notification Details page.
- **Showing Related Notifications** – On the External Notification Details page, if there were multiple results for a file analysis, a **Related Notifications** link in the Related Views menu opens the External Notifications table filtered for files with the same MD5 hash.
- **SHA-256 Reporting in Notifications** – The External Notifications table now includes a **Malware SHA-256** column to indicate when a SHA-256 hash is reported in a Palo Alto Networks notification.
- **Multiple Analysis Results for a File Submitted to WildFire** – For files submitted from Parity Server to WildFire for analysis, the Analyzed Files tab on the Requested Files page can show that WildFire provided analysis results from two or more environments.

Note: The External Notification Details page includes a Version field that reports on the version of the external appliance or service that provided the notification. This value is whatever the external source chooses to provide in its XML output, and does not necessarily map directly to product version. For example, WildFire 6.0 notifications provide the WildFire API version number, currently 2.0.

Mac OS X 10.9 (Mavericks) Support and Anti-Virus Software

If you run anti-virus software, you should exclude the Bit9 agent installation directories from anti-virus scanning. If you are running OS X 10.9 (Mavericks) or later, the location of the Bit9 *kernel extension directory* has changed. For Mavericks and later, exclude **/Library/Extensions/b9kernel.kext** from scanning.

For earlier OS X releases, you can use the kernel extension path documented in the ""Managing Computers"" chapter of the *Using Parity* guide. All of the other Bit9 directories remain the same for all OS X versions.

Corrective Content

If you are upgrading from Parity v6.0.2 or v7.0.0, note that this release of Parity v7.0.1 addresses all of the relevant issues that have been addressed in v6.0.2 and v7.0.0 patch releases to date. Each release includes general improvements in product quality, based on our ongoing testing of Parity v7.0.1.

Corrective Content in Parity 7.0.1 Release (Build 2612 Patch 21)

- Windows API allows users running agents in High Enforcement to bypass execution blocks [43924].
  - 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 Parity 7.0.1 Release (Build 2496, Patch 20)

- An invalid trusted publisher rule was created and not detected by the console [39307].
  - Details: A publisher rule could be created that would result in configuration list (CL) errors. The invalid CL entry would cause an error when a CL update was sent to the agent. In this release, the publisher rule does not create invalid CL entries.
  - Applies to: Agent

- Windows crashed on several computers after upgrading to from 7.0.1 to 7.2.0 Patch 4 [42006]
  - Details: During some upgrades and uninstalls, Windows could crash with dump files containing the error message "Driver_Unloaded_Without_Cancelling_Pending_Operations". In this release, pending operations are cancelled before the driver is unloaded and the error condition no longer occurs.
  - Applies to: Agent

- Console intermittently shows endpoints as connected/disconnected [42208]
  - Details: If an agent uploaded a binary file containing a badly formed certificate or if the server received a file certificate not supported by the Windows CryptoAPI, the server would repeatedly try and then fail to validate this certificate. This would cause the server log to balloon rapidly with error messages and the endpoints to intermittently be connected and disconnected. In this release, the badly formed certificate is rescheduled for validation at a later time in the same manner as other erroneous certificates, which prevents the multiple validation failures.
  - Applies to: Server

Corrective Content in Parity 7.0.1 Release (Build 2414, Patch 19)

- Need to allow publishers whose names differ only by case [39188].

- Details: If files had a publisher name that differed only in case from the trusted publisher name, those files were not being approved. In this release, if a publisher is approved, all files from publishers with that publisher name are approved, regardless of the case of the name."
- Applies to: Server

- Error collecting diagnostics from Mac agents [40873].
  - Details: When capturing diagnostics data on a Mac agent using "b9cli –capture" some logs were not captured. In this release, all necessary logs are now captured by the "b9cli –capture" command on Mac agents.
  - Applies to: Agent

- SQL server CPU consistently has high utilization due to FireEye integration [40937]
  - Details: CPU utilization exceeded 100% at times when FireEye analysis was requested. In this release, database improvements were made to reduce the CPU usage.
  - Applies to: Server

- Invalid exclusion rule could lead to lack of file tracking on the server [41306].
  - Details: Due to insufficient parsing of an exclusion rule, file tracking could be halted on the server. In this release, the server and agents will ignore poorly formatted exclusion rules that have a missing or extraneous semi-colon and file tracking will not be halted.
  - Applies to: Server

- Error message when filtering by 'Computer Name' in the Approval Requests section of the server console [41771].
  - Details: When filtering for 'Computer Name' using the options 'is', 'is not' and 'begins with', the following error occurred: "Invalid field:Computer". In this release, using these filter options produces no error.
  - Applies to: Server

- Poor performance on DFS shares when agent is in most policies [41803].
  - Details: Saving .xlsx files to DFS shares resulted in poor server performance. In this release, changes in caching file permissions when working with network shares solved the performance issue.
  - Applies to: Agent

Corrective Content in Parity 7.0.1 Release (Build 2327, Patch 18)

- Error 500 from server System Configuration/General [40617]
  - Details: When Bit9 SQL service account lacked permission "View Server State", the System Configuration/General page returned error 500. In this release, the error no longer occurs.
  - Applies to: Server

- Files within .7z archives in a trusted directory are not added to the Bi9 file inventory [40717]
  - Details: Archives with ".7z" extension within a trusted directory contained interesting files but those files were not classified as interesting. In this release, those files will be classified as interesting.
  - Applies to: Server

- Notifier is not showing on Win 2003 server [40760]
  - Details: When the Parity agent ran on the Windows 2003 server, disabling the Windows Terminal Server (WTS) caused the Parity agent to lose session information, which prevented the Parity notifier from being displayed. In this release, a new internal mechanism is employed to allow the notifier to be displayed whether the WTS is disabled or not.
  - Applies to: Agent

- Agent crashed during initialization[40782]
  - Details: Under certain circumstances, an internal operation to collect service metadata during agent initialization would free too much memory causing an agent crash. The crash does not occur in this release.
  - Applies to: Agent

- High CPU utilization when interacting with Symantec Endpoint Protection [40887]
  - Details: In 7.0.1 P17 and earlier, an interaction between Symantec Endpoint Protection and the Bit9 Agent could cause use high CPU usage when the Bit9 agent woke from sleep. In this release, the issue has been resolved.
  - Applies to: Agent

Corrective Content in Parity 7.0.1 Release (Build 2254, Patch 17)

- File Propagation Alert processing degrades performance [40501]
  - Details: Excessive disk I/O was being spent in processing "File Propagation Alerts" which took significant SQL disk resources. This led to slower overall performance. In this release File Propagation Alerts no longer degrade performance.
  - Applies to: Server

- Needlessly analyzing .jar files when the script rule for java is disabled [40016]
  - Details: During file analysis, .jar files were being classified as interesting files and tracked in the agent's file inventory even when the script rule for java was disabled. In this release, newly analyzed .jar files are not classified as interesting if the .jar script rule is not enabled. Any .jar file already in the agent's inventory will continue to be tracked as "interesting" until the file is re-analyzed. (See Known Issue **Error! Reference source not found.**)
  - Applies to: Agent [Windows]

- System crash seen on endpoints running Citrix's Personal vDisk [40360]
  - Details: A system crash could occur when the Bit9 agent and Citrix Personal vDisk were installed. In this release, the problem is resolved.

- Applies to: Agent [Windows]

- Cache Consistency Check after every Agent Restart [40081]
  - Details: The agent would unnecessarily rescan the disk after each agent restart which led to more resource usage by parity.exe and decreased system performance. In this release, the unnecessary rescans do not occur.
  - Applies to: Agent [Windows]

- Agent startup delay [40556]
  - Details: During agent startup, some implementations were found to be unnecessarily time consuming. These were corrected and agent startup time was improved.
  - Applies to: Agent [Windows]

- Event reports on dashboards do not open correct event filters [40277]
  - Details: The links on the Event Reports dashboard portlet did not load the correct saved views on the Reports->Events page. The issue has been corrected.
  - Applies to: Server

- Decreased available memory can hang the system [40593]
  - Details: Loss of available memory was reported which could lead to eventual system crash. A small memory leak was fixed in this release to correct the problem.
  - Applies to: Agent {Windows]

- .zip files not getting uploaded by FireEye [40553]
  - Details: Failed file analysis requests for files submitted to FireEye would accumulate in the server database, causing performance issues and delay in deleting analyzed files from disk. Files from failed analysis requests are now purged.
  - Applies to: Server

- Bit9 server install fails due to error in certutil.exe. [39958]
  - Details: During Bit9 server installation, the install failed with error “failed on executing certutil.exe during Bit9 server install”. The handling of special characters in SQL passwords has been corrected to resolve the issue.
  - Applies to: Server

- Parity.exe consuming more than 400M of memory [39954]
  - Details: If many files were opened for write access but never written to, the agent’s memory usage would increase over time until either the agent was restarted or resources were exhausted. In this release, the issue has been eliminated.
  - Applies to: Agent [Windows]

- Error resetting File Propagation Alert [40311]

- Details: Attempts to reset file propagation alert resulted in the error “Failed to reset alert”. The Bit9 Reporter log showed multiple instances of the error “Database timeout expired: AlertExecute’. The Reporter service is now temporarily stopped while resetting the alert, eliminating the errors.
- Applies to: Server

- Server initiates Agent upgrades even when policy based upgrade flag is disabled [40199]
  - Details: When Disable Upgrades was selected from the Action menu on the Policies page and applied to one or more policies, the agents in these policies were still upgraded if Automatic Agent Upgrades was then enabled on the System Configuration page Advanced Options tab. In this release, this no longer occurs.
  - Applies to: Server

Corrective Content in Parity 7.0.1 Release (Build 2139, Patch 16)

- Device approval request providing no actionable information [39626]
  - Details: When a notifier was displayed for a block due to executing from an unapproved device, and an approval request was submitted via this block, the approval request in the console showed no actionable data. In this release, when a file is blocked from executing from a banned or unapproved device, the notifier will no longer display an approval request.
  - Applies to: Server

- When upgrading to Apple OSX 10.9.4 some operating system files were not getting promoted [40149]
  - Details: During OSX operating system upgrades, some system files may were not getting promoted, causing files to be unapproved and causing the upgrade not to succeed. Code has been changed to fix the promotion problem.
  - Apples to: Agent [Mac]

- Zip files were not getting uploaded to FireEye [39176]
  - Details: When uploading an extremely large number of files to FireEye, an exception was generated causing the zip file uploads to fail. In this release, the exception is no longer generated and the uploads are now successful.
  - Applies to: Server integrations with connectors

- Cleanup of deleted uploaded files [39965]
  - Details: When there were many uploaded files scheduled to be deleted on the Bit9 server, the Server would stop sending policies for an extended period. In this release, the cleanup of uploaded files has been modified to correct the problem
  - Applies to: Server

- FireEye version 7.2 Integration with Bit9 was not working [39924]

- Details: The XML format changed in version 7.2 of FireEye. This caused a FireEye event "FireEye exeprtion: Unauthorized post attempt" which prevented FireEye appliance from receiving external notifications. In this release, the Bit9 Server has been modified to accommodate the format change.
- Applies to: Server integrations with connectors

- Server Patcher does not report when Connector MSI fails to upgrade [39944]
  - Details: In previous patches, the Bit9 Connector upgrade did not echo its log file into the main patch log file, nor did it show on screen. The Connector's upgrade log will now appear in the console as well as in the main log file for the patch process.
  - Applies to: Server Installer

- Bit9 uses 99% of MAC CPU after upgrade [40051]
  - Details: An error causing some file paths to get duplicated parts impacted computer performance by causing backup failures whose frequent retries caused CPU to spike. In this release, a fix has been made to get the path parts correctly.
  - Applies to: Agent [Mac]

- Not receiving external notifications from PAN if Initial Import is set to 0 [38832]
  - Details: External notifications from Palo Alto Networks devices were not received by the Bit9 Server if the initial Import parameter was set to 0. In this release, setting the Initial Import parameter to zero does not prevent new notifications from arriving.
  - Applies to: Server

- In the events tab, the auto-complete list for File Path points to the Device Catalog [39648]
  - Details: Auto-complete for file path filtering on the Events page in the Bit9 Console was linked to device listing instead of file paths. In this release, auto-complete for the file path filter on the Events page correctly points to file paths
  - Applies to: Console

- Agent config only accepts 6 digit host id [39618]
  - Details: The maximum length of Host ID was previously limited to 6 digits in the details page of items on the agent configuration page, agent_config.php, accessed from the console. In this release, the maximum length Host ID field on the agent configuration details page has been increased from 6 digits to 10 digits so that it can accept the full range of possible Host IDs.
  - Applies to: Console

Corrective Content in Parity 7.0.1 Release (Build 2053, Patch 15)

- Approval request alerts were not firing for rapid requests [37861]
  - Details: Approval request alerts are now generated each time criteria is met without grouping of approval requests occurring more than once every 20 seconds.
  - Applies to: Agent [All]
- SCCM server crash, unable to load image [38595]

- Details: Added configuration option to disable watchdog timer which resolved this specific problem
- Applies to: Agent [Windows]

- File uploads were stuck in “acquiring file” status [38650]
  - Details: Problem occurred on one specific server and was fixed by improved error handling to previous fix.
  - Applies to: Agent
- FireEye reports were indicating first started process as the malware [38650]
  - Details: First started process reported in FireEye reports is usually the actual malware being analyzed (detonated) and is being used as the top level malware hash, in case when there are no other top level malware hashes.

    In case of web-infection notifications, the first process is not always the malware, so this could lead to identifying processes such as AcroReader and Cmd as malware. This is now fixed so that such assumption is not used any more for notifications of type other than "malware-object"
  - Applies to: Agent [All]
- Time zone conversion error when parsing date/time from PAN logs [38770]
  - Details: The bug is with the time zone mapping. Time zone is used to convert local time stamp from the PAN appliance to the UTC timestamp, used by the Bit9 database.

    US/Central zone was mapped by mistake to Central Standard Time (Mexico) instead of just CST. Since Mexico had Daylight savings switch happen on 6th Apr at 2am->3am, the code produced an exception that timestamp between 2am and 3am could not exist. Code fixed to handle exceptions.
  - Applies to: Agent [All]
- File uploads to FireEye for analysis had timeouts and poor performance[38792]
  - Details: Added missing SQL index to improve file upload performance
  - Applies to: Agent
- FireEye timeout was set to SQL timeout [38793]
  - Details: FireEye timeout changed to not use SQL timeout. Avoids potential for infinite timeout limit. SQL timeout modified to 300 seconds to fit web request timeout. Both timeout parameters are now configurable from the web configuration file.
  - Applies to: Agent
- Agent health check reported false errors [38806]
  - Details:
    - During the Agent health check, there were two errors reported:
      - "The Parity Kernel is not a registered Driver"
      - "Parity is not a registered Service."
    - In fact, the Parity Agent and Kernel driver were running and registered services.
    - The problem involved misinterpreting results from a large number of registered services and has now been fixed.
  - Applies to: Agent [All]
- Internet Explorer 11 was incompatible with Bit9 Security Platform patch 13 [38878]
  - Details: The user should consult the documentation to determine which browsers are supported for each release.
  - Applies to: Agents and Server [Windows]
- Rare fatal error on login after upgrade [38896]

- Details: Fixed an upgrade bug which in rare situations could cause the corruption of parity.ini during upgrade
- Applies to: Agent [All]

- Improvements to Active Directory Policy Switching [38945]
  - Details: In some circumstances, especially when certain types of VPN were in use, the Bit9 agent would not correctly switch Active Directory mapped policies based on user membership in Active Directory groups. This release provides mechanisms to force the agent to re-evaluate group membership. Please contact Bit9 Support if you need more information.
  - Applies to: Agent [Windows]
- Server inventory processing halts [39066]
  - Details: Fixed issue where server inventory processing could possibly stop if corrupt host ID found.
  - Applies to: Server
- Slow agent installation [39247]
  - Details: Agent installation speed improved by better treatment of cached script execute reads
  - Applies to: Agents [all]
- SQL injection in the web interface [39543]
  - Details: Several security issues affecting the security of the Bit9 console were addressed in this release.
  - Applies to: Server [all]
- Performance slowness in SQL database interaction [38812]
  - Details: The handling of certain SQL errors and nesting of some SQL queries were causing performance issues. Fixed in server database interaction.
  - Applies to: Server [all]

Corrective Content in Parity 7.0.1 Release (Build 1964, Patch 14)

- Java class files appearing in inventory when Java tracking disabled [34941]
  - Details: In previous releases, Java class files would appear in the file inventory, even when Java tracking was disabled. In this release, class files do not appear in the inventory unless Java tracking is enabled.
  - Applies to: Agent [All]
- Mac agents receiving many unnecessary requests for metadata [35381]
  - Details: When agents on Mac systems reported their file inventory to the server, the server sent many unnecessary requests for metadata, such as MD1 and SHA1 hash values. In this release, the number of metadata requests has been reduced, improving agent performance.
  - Applies to: Server and Mac agents
- Cache consistency check is reported unsuccessful [37805]
  - Details: When an agent is upgraded, it can sometimes initiate a cache consistency check as a result of the upgrade. If another CC is initiated during the initial cache check, the first CC complete event would report that the initial CC was unsuccessful before starting the second CC even though the first CC actually completed successfully.

  - Applies to: Agent [All]
- Config List version is blank in CSV export [37845]
  - Details: When Events show the column for CL Version, values are displayed, but when these events are exported to a CSV file, the CL version is shown as blank.
  - Applies to: Server
- Slow performance on agents cloned using VDI environment [38018]
  - Details: When using VDI environment to clone computers with Bit9 agents initialized, if the user logged out but did not undeploy the VM, the VM reverted to the previous snapshot. When the agent logged back in, the agent had to resync for going back in time. This impacted the performance of the agents.
  - Applies to: Server
- Archive logs consume large storage space [38214]
  - Details: Bit9 Agents occasionally sent the server erroneous file hashes, which would get logged. This erroneous data could cause significant growth in the size of the logs. This release eliminates the condition that caused the erroneous hashes to be sent.
  - Applies to: Server

Corrective Content in Parity 7.0.1 Release (Build 1892, Patch 13)

- File uploads require additional system configuration permissions [37516]
  - Details: In addition to the appropriate file upload permission, *Manage system configuration* permission was required to allow console users to upload files from agents. In this release, *Manage system configuration permission* is not required to upload files.
  - Applies to: Server
- Device approvals and bans not working for multiple device serial numbers [36457]
  - Details: When a device with multiple serial numbers was approved or banned on the server, the approval or ban was not effective on the agent. In this release, such approvals and bans are applied to all of the specified devices.
  - Applies to: Agent [Windows]
- All results blocked if AD mapping query returns too many results [37682,37186,37438]
  - Details: On the Policies/Mappings page, a query in the AD mapping interface is limited to no more than 500 results (e.g., users or groups). Previously, if more than 500 items were found, none of the results would be displayed. In this release, if more than 500 results are found, the first 500 will be displayed and a message will indicate that the results exceeded the limit. Contact Bit9 Technical Support if your site requires handling of more results than this.
  - Applies to: Server
- Show/Hide Filter link not working on Processed Events panel [36906]
  - Details: On the Edit Event Rule page, the Show/Hide Filter link in the Processed Events panel did not open the Filters interface. This release corrects the issue.
  - Applies to: Server
- Notifier not displaying on Windows 2003 systems using Windows Terminal Services [36258]
  - Details: On Windows 2003 systems using Windows Terminal Services, the blocked file notifier did not always display when Bit9 blocked a file. This release corrects the issue.
  - Applies to: Agent [Windows]

- New bans not enforced when same process executes file on Mac agents [28998]
  - Details: If existing rules allowed a file to execute and then more restrictive rules were activated that should have blocked it, the file would not be blocked if executed by the same process that ran it previously. In this release, switching to rules that should ban file execution will apply the ban shortly after the new rule is received from the server, even if the same process is attempting the execution.
  - Applies to: Agent [Mac]
- Mac agent cache increasing to unbounded size [37965]
  - Details: Previously, Mac agent caches could grow very large in size. In this release, events and files already sent to the server are pruned, reducing cache growth.
  - Applies to: Agent [Mac]
- Files discovered in Low Enforcement appear as *Unapproved (Persisted)* [37589]
  - Details: Files discovered by Mac agents during Low (or no) Enforcement were assigned a Local State Detail of *Unapproved (Persisted)* on the server, even though this should not occur at these levels. In this release, such files are assigned a Local State Detail of *Unapproved*, indicating that they may be locally approved on Enforcement Level change to Medium or High.
  - Applies to: Agent [Mac]
- Failure to open a file for analysis causes CPU spike [35759]
  - Details: When Parity is unable to open a file for analysis, it re-queues the file for delayed analysis. On rare occasions, this delay could become zero, leading to constant attempts to open the file and using a significant percentage of CPU resources. In this release, the delay before resubmitting a file is managed to avoid this situation.
  - Applies to: Agent [Windows]
- Certificate recalculation could cause UI and upgrade timeouts [37477]
  - Details: When the Bit9 Server managed a large number of digitally signed files, changing the Certificate Options on the System Configuration/Advanced Options page could cause a timeout in the console because of certificate state recalculation. This could also occur during patch upgrades in which certificate settings changed. In this release, improved handling of certificate recalculation reduces the likelihood of a timeout.
  - Applies to: Server, Patch/Upgrade Installer
- Actions with multiple report rules only trigger one report [36706]
  - Details: In previous releases, actions on an agent could only trigger one report rule, even if multiple rules requested that events be reported for that action. In this release, an execute or write action can trigger up to 10 report rules.
  - Applies to: Agents [All]
- Agent crash during initialization [37463]
  - Details: In some cases, agents could crash during initialization due to accessing uninitialized memory. This release addresses that issue.
  - Applies to: Agent [Windows]
- Agent configuration list not updating [37095]
  - Details: In some cases, an agent would stop updating its configuration list, and so would not have the latest rules provided by the server. The condition that caused this issue has been eliminated.
  - Applies to: Agent [All]

- Alert processing causes performance issues [37322]
  - Details: Security Alert and File Propagation alerts could cause degradation of server performance, including console timeouts and growth of the file backlog. This problem has been resolved.
  - Applies to: Server
- Requests for file analysis are stuck in "Acquiring file" status [37354]
  - Details: With the Bit9 Connector, when a request was made to send many files from one endpoint to an external analysis service, the file uploads could become stuck in the “Acquiring file" state. This release corrects this issue.
  - Applies to: Server
- Some Event page queries cause slow performance or console time-out [37384]
  - Details: Depending upon filters used and the number of results, certain queries on the Events page could cause slow console performance or time-outs. In this release, the performance of queries involving common event filter fields, including Source, Policy, Type and Subtype, has been improved.
  - Applies to: Server
- Processing of file inventory backlog is slow [37541]
  - Details: The processing of file inventory by the server could become increasingly slow when the backlog of individual agents is very high. The efficiency of inventory backlog processing has been significantly improved in this release.
  - Applies to: Server
- Upgrade from v6.0.2 to v7.0.1 fails [37771]
  - Details: When a v6.0.2 server included a large number of rules with long paths, attempts to upgrade the server to v7.0.1 could fail. This release eliminates this upgrade failure condition.
  - Applies to: Server
- Parity Knowledge/SRS connection loss causes high volume of Windows event warnings [36335]
  - Details: Interruption of the connection between the Bit9 Server and the Parity Knowledge/SRS server caused a very large daily volume of Windows event warnings to be logged. In this release, events still warn about connectivity issues but the number of events generated in this case was reduced to decrease the impact on the event logging system.
  - Applies to: Server
- FireEye exception when processing multiple notifications simultaneously [37175]
  - Details: With Bit9 Connector enabled, if a FireEye appliance box sent multiple notifications to the Bit9 Server at the same time, some notifications could fail to reach the server. In this case, the Bit9 Server showed the error "Fireeye exception: The process cannot access the file 'C:\Program Files (x86)\Bit9\Integrations\FireEye\listener\store\...". The issue that caused the notification loss and error message has been corrected in this release.
  - Applies to: Server
- Bit9 Console not accessible (404 error) after upgrade from v6.0.2 on Windows 2003 [36714]
  - Details: On systems running Windows 2003 SP2 with IIS6, server upgrades from v6.0.2 to v7.0.1 would complete successfully, but the console would fail to open, showing an IIS 404 error. This was due to failure to update IIS with ‘FastCGI’ included in its configuration. In this release, upgrades from v6.02 on this platform no longer encounter this problem.
  - Applies to: Server

- Error messages not handled correctly for invalid PAN appliance credentials [37478]
  - Details: With the Bit9 Connector enabled for Palo Alto Networks, if unsupported special characters, such as the colon (:) were used in the PAN appliance password, they would not be trapped by the console validation process, and a misleading error appeared in the PAN logs. In this release, the correct error, "Invalid credentials", is displayed and is reported in the console as well as the log files.
  - Applies to: Server
- Notifier tag <NotifierBroadcastSystem> does not work correctly [36995]
  - Details: The notifier tag *<NotifierBroadcastSystem:User|Group|blank>* , which should determine how notifiers are displayed in a session virtualization environment, was not working correctly. In this release, it functions as documented.
  - Applies to: Agent [Windows]
- Patch upgrade is very slow [37084]
  - Details: The server patch upgrade process creates approvals for all files shipped in the patch. In previous releases, the process of creating approvals for these files was slow, resulting in longer than expected installation times. The approval process has been optimized in this release for faster upgrades.
  - Applies to: Server
- Global CLI Password Update Doesn't Propagate to 7.0.0 Agents [37406]
  - Details: When a global agent management password was set in v7.0.1, it was not effective on any 7.0.0 agents connected to the server. In this release, the password will be effective for both 7.0.0 and 7.0.1 agents.
  - Applies to: Agents [All]
- Console reports fatal SOAP error and agent connections are lost [37481]
  - Occasionally, the Bit9 Server could become deadlocked, which would prevent agents from connecting to the server. This release fixes this issue.
  - Applies to: Agents [All]

Corrective Content in Parity 7.0.1 Release (Build 1807, Patch 12)

- Crash on CentOS after Bit9 platform install [37482]

Corrective Content in Parity 7.0.1 Release (Build 1679, Patch 11)

- Tamper protection blocks installation of Java and other Mac OS X components [36290]
  - Details: Bit9 tamper protection was blocking installation of Java and OS X system updates on agent systems. In this release, these components are allowed to install.
  - Applies to: Agent [Mac]
- Agent scanning of real-time file-system events causes kernel panic [35244,36323]
  - Details: Under rare circumstances, a kernel panic occurred when Parity scanned real-time file-system events. In this release, such scans no longer cause a kernel panic.
  - Applies to: Agent [Mac]

- Agent cache corruption not automatically fixed [36146,36156,36755]
  - Details: Under some circumstances, the agent could be prevented from automatically fixing certain cache integrity issues during startup. This release corrects the problem, which also improves agent startup time and reduces the use of system resources during startup. If the agent finds and resolves a problem with the cache, the following messages appear:
    - Parity Agent had to rebuild its primary cache and now has to re-initialize
    - Parity Agent had to restore its primary database cache

    Note: New commands have been added to the Advanced menu of the Computer Details page to allow a remediation response from the console if an agent's cache becomes corrupt and automatic remediation is not possible. These commands should be used only in conjunction with Bit9 Support.
  - Applies to: Agent [Windows]
- Server stops processing agent messages or agents drop offline [36665, 36196, 36503]
  - Details: In some situations, the Bit9 server could stop processing agent connections due to internal server deadlocks, requiring a restart of the ParityServer service. This issue has been addressed in this release.
  - Applies to: Server
- Event logs display globalroot instead of DOS file path [36202]
  - Details: On the console Events page, process names sometimes were displayed in NT namespace format (\\?\globalroot\harddiskvolumeX\folder\...). In this release, process names are correctly displayed in DOS format (c:\folder\...).
  - Applies to: Server and Agent
- Slow loading of External Notifications page [36429]
  - Details: The External Notifications table page was slow to load when it had a large number of notifications. Performance of the External Notifications page has been improved in this release.
  - Applies to: Server
- Incomplete information in some configuration lists sent to agents [36466]
  - Details: In some cases, the configuration list sent by the server to agents did not contain all of the current information (rules, settings, approvals, etc.) that should have been sent. This release corrects the problem that caused this.
  - Applies to: Server
- Bit9 installer and patcher fail when default database schema is not dbo [36537]
  - Details: Prior versions of Bit9 required that the default schema of the database user used for installation and upgrade be "dbo". This is no longer required.
  - Applies to: Server
- Fatal error when installing Bit9 server on a system with only SQL 2012 runtimes [36559]
  - Details: When installing the Bit9 server on a system with only a fresh installation of SQL 2012 native client and command line tools (i.e., previous SQL versions were never present), the installer could not properly detect and make use of the SQL 2012 tools. This would cause a fatal error during server installation. This release includes changes to help detect the required tools in SQL 2012 when they are installed in the default location.
  - Applies to: Server
- Security alerts cause database performance degradation [36565]

  - Details: In previous releases, evaluation of Computer Security Alerts could cause high database usage and degraded server performance. This release improves the efficiency of such evaluations.
  - Applies to: Server
- Upgrades from 6.0.2 to 7.0.1 disconnect the server from Parity Knowledge Service [36696]
  - Details: In some cases, server upgrades from v6.0.2 to v7.0.1 would break the connection between the Parity Server and the Parity Knowledge Service, and would not allow re-entry of the Parity Knowledge key to re-establish the connection. In this release, the key may be re-entered if necessary.
  - Applies to: Server
- Agent version not updated in console after upgrades from 7.0.0 HotFix [36668, 36754]
  - Details: After agents were upgraded to v7.0.1 from a 7.0.0 HotFix, the console still showed the 7.0.0 HotFix version for the agents. In this release, the console shows the new version number for agents upgraded from a 7.0.0 HotFix.
  - Applies to: Server
- Initialization is interrupted by cache consistency scans [36873]
  - In v7.0.1 Patch 9, initialization could be cancelled if additional cache consistency scans were scheduled while initialization was still in progress. Restarting the agent would resume the initialization process. In this release, initialization is not interrupted in this case.
  - Applies to: Agent [Windows]
- Improvements in console security [36840]
  - Details: Several security issues affecting the security of the Bit9 console were addressed in this release.
  - Applies to: Server

Corrective Content in Parity 7.0.1 Release (Build 1631, Patch 10)

- None

Corrective Content in Parity 7.0.1 Release (Build 1561, Patch 9)

- Blocked Files (All) view does not display expected results [34457]
  - Details: The Blocked Files (All) Saved View on the Events page might not show any events even though there are Blocked File events. Other file-related event views might also incorrectly show no data. In this release, the underlying cause of this problem has been addressed.
  - Applies to: Server
- Problems when systems are rebooted during initialization [34810]
  - Details: Rebooting a system before file initialization has completed might result in long startup delays, problems logging in, or reports of unanalyzed blocks for systems in medium and high enforcement. This release corrects the deadlock that could occur and allows initialization to resume upon restarts.
  - Applies to: Agent [Windows]

- Temporary override required Manage Computers permission [35086, 35032]
  - Details: In previous v7.0.1 releases, users required both Manage Computers and Temporary Assign Computers permissions to generate a temporary policy override code for a computer even though v7.0.0 only required the Temporary Assign Computers permission. This release modifies access control so that only Temporary Assign Computers permission is needed.
  - Applies to: Server
- Trusted Updater for WebEx might not allow WebEx updates [35206]
  - Details: In some cases, enabling the Updater for WebEx did not allow WebEx updates to successfully install because of problems with temporary files. This release addresses the problem.
  - Applies to: Agent [Windows]
- Certificate handling for trusted publishers differs from v7.0.0 [35242,35241,35011]
  - Details: Parity v7.0.1 included changes to the requirements for certificate validity (such as minimum key length and supported signature algorithms) that might result in failures to approve files that were previously approved in v7.0.0. This release restores similar defaults and provides the ability configure these settings on the Advanced tab of the System Configuration page.
  - Applies to: Server
- Event pruning and Parity Knowledge synchronization might not complete [35416, 35419]
  - Details: Errors that occurred during event pruning could cause pruning tasks to never complete and might cause Parity Knowledge synchronization to be delayed. This release addresses the underlying deadlock that could affect these activities.
  - Applies to: Server
- Some publishers are not being discovered following an upgrade from v7.0.0 [35425]
  - Details: Publishers and their underlying certificates are supposed to be re-evaluated following an upgrade to ensure information related to new controls and policy options can be applied, but this was not being done under all circumstances. This release ensures that publisher information is updated following an upgrade.
  - Applies to: Agents [Windows]
- Agents might be missing policy settings when using clones of customized policies [35433]
  - Details: When a new policy was cloned from a policy that had customizations of Advanced Settings, the cloned policy might not send the customized Advanced Settings to its agents. This would occur when reputation approvals were enabled for the policy. In this release, all settings from cloned policies are sent to agents, regardless of source policy customizations or the reputation setting.
  - Applies to: Server
- Events might not be displayed when applying a filter by computer [35437]
  - Details: Filtering events by computer on the Events page could cause the console to perform slowly or time out. The underlying filtering issue has been addressed for this release.
  - Applies to: Server
- Events might not be displayed from systems with significantly incorrect time setting [35774, 35459]
  - Details: In previous releases, an event from an agent would not be processed if the system time on the agent was set to distant time in the past or future. This issue has been addressed in the current release.

- Applies to: Server

- Files signed by a trusted publisher might not be approved [35521]
  - Details: In previous releases, certificate validation might have required access to intermediate certificates that are not present in the system certificate store. This could result in validation errors and failure to approve files by publisher for all files discovered after the publisher certificate was first discovered. This release removes the dependency on intermediate certificates in the certificate store and will approve files that may have been incorrectly unapproved in prior releases. See Control of Certificate Restrictions on page 9 for related configuration options.
  - Applies to: Agent [Windows]
- Countersignatures were not being validated even when present in some circumstances [35603]
  - Details: If the Bit9 Agent was configured to not require countersignatures, they would be ignored even when present. This release corrects the behavior so that countersignatures are validated when present, but it does not require they be present for the signature to be validated. See Control of Certificate Restrictions on page 9 for related configuration options.
  - Applies to: Server, Agent [Windows]
- Internet Explorer 8 is not able to save or export all columns in views [35680]
  - Details: When the console was accessed with IE8, changes to the columns shown in a Saved Views would not be saved in the view, and exporting the data to a CSV file would export only the data from the default columns. This issue has been corrected.
  - Applies to: Server
- Notification of block events may take 20-30 seconds to appear [35791]
  - Details: When a reputation-based approvals are enabled, agents might not display the Notifier for up to 30 seconds if the Bit9 server was unable to look up reputation information in Parity Knowledge. This release corrects the unnecessary timeout in this case.
  - Applies to: Server
- Console searches by hash are slow and may timeout [35901]
  - Details: Searching for hashes in the console performed slowly. In this release, filtering by file hash (MD-5, SHA-1, and SHA-256) has been optimized.
  - Applies to: Server
- Server upgrades using SQL Server 2005 may fail [35972]
  - Details: When a non-standard port was used on the Bit9 Server for file uploads with SQL Server 2005, upgrades might fail with the error “Subqueries are not allowed in this context. Only scalar expressions are allowed.” This is corrected in this release.
  - Applies to: Server
- Incorrect description of installer analysis in trusted directories [35565,35831]
  - Details: Previous versions of the *Using Parity* guide and online help incorrectly described the treatment of Windows installer files (such as MSIs) in trusted directories and implied that all files in the MSI are approved in advance. The trusted directory documentation in this release correctly describes that only the Windows installer itself is approved via the trusted directory.
  - Applies to: None
- Script rules might not work when using associations referencing processors with “Program Files” or “Program Files (x86)” in path [35926]

- Details: If a file association was chosen as the process value in a script rule definition and the process associated with the file extension in the script rule definition contained a space in its path, script executions might not be detected. This release corrects this issue.
- Applies to: Agent [All]

Corrective Content in Parity 7.0.1 Release (Build 1460, Patch 8)

- Improvements in Console Security [33227, 35037, 35038]
  - Details: Several security issues affecting the security of the Parity console were addressed in this release.
  - Applies to: Server
- Event for Report-only Memory Rules does not Contain Requested Access Rights [34127, 34132]
  - Details: Occasionally, events reported for report-only Memory Rules would contain a blank or improperly formatted "Requested Access Rights" section. This release displays the correct access rights.
  - Applies to: Agent [Windows]
- Stop Error "System Thread Exception Not Handled" [34745, 34786, 34942, 35133, 35167]
  - Details: In rare circumstances, a Stop Error "System Thread Exception Not Handled" would occur. This release addresses the underlying issue.
  - Applies to: Agent [Windows]
- Stop Error on Systems with McAfee Endpoint Encryption [26039, 35082, 35116, 35323, 35248]
  - Details: A Stop Error occurred when the Bit9 agent was installed on a system that had McAfee Endpoint Encryption installed. This release allows correct interoperability between Bit9 and McAfee Endpoint Encryption.
  - Applies to: Agent [Windows]
- Stop Error on Windows 8 [35151]
  - Details: In some circumstances, a Stop Error would occur on Windows 8 due to incorrect access to registry data. This Stop Error is addressed in this release.
  - Applies to: Agent [Windows]
- Stop Error 0x0000007F on Windows 2003 and 2008 Server [34746, 35063]
  - Details: In rare circumstances, a Stop Error with the code 0x0000007F (*UNEXPECTED_KERNEL_MODE_TRAP*) would occur when there were Custom Rule changes during agent startup. This Stop Error is addressed in this release.
  - Applies to: Agent [Windows]
- Performance Issue with Rule Evaluation [33999, 35216]
  - Details: When processes quickly started and exited and used many different user accounts, the Bit9 agent would re-evaluate Custom Rules too frequently. This caused performance issues on affected endpoints. This release ensures that rules are evaluated less frequently and improves agent performance.
  - Applies to: Agent [Windows]

- Enhanced Access to Certificate Parameters [35011, 35097, 35187, 35241]
  - In v7.0.1, certificates used for approval of a file by publisher may be required to meet specifications for minimum key length and signature algorithm. For new installations starting with Patch 8, the default certificate values are a minimum key length of 1024 and exclusion of the *MD2RSA* algorithm from use in approvals. For installations that are upgraded to Patch 8 (or later) from either prior patches of 7.0.1 or from earlier versions, the default minimum key length is 512 and no algorithms (of the 4 listed) are excluded. These settings may be modified on the "Advanced Options" tab of the System Configuration page.
  - Applies to: Agent [Windows], Server
- Deadlock on Interaction between Bit9 Agent and Third-Party Products [35330, 35341]
  - Details: In circumstances where other kernel-based products were installed on the same system as the Bit9 agent and the agent was attempting to obtain the name of a file system, a deadlock could occur. This release addresses the underlying cause of the deadlock. Note that the deadlock may still occur entirely within the other products, even when this fix is in place.
  - Applies to: Agent [Windows]
- Server Upgrade Can Cause Alerts to be Re-sent [34428, 35292, 35300]
  - Details: In previous releases, the server upgrade process reset information about background tasks, which could cause them to be re-processed. Re-processing could lead to previous Alerts being re-sent and other background tasks running more than once. This release correctly preserves the information on the state of background tasks.
  - Applies to: Server
- "Certificate Checked" Event does not Display Certificate Name [34912]
  - Details: In some circumstances, the "Certificate Checked" event in the Bit9 console would not display the associated certificate's name. This release improves the display of this event. Note that there are still some limited circumstances in which the console does not have access to the name and in those cases, the certificate identifier will be displayed.
  - Applies to: Server
- Installation from Network Fails [28721, 34449]
  - Details: In rare circumstances, software installations from a network drive failed while attempting to execute external components. This release improves the tracking of file operations on network file systems, allowing these installations to succeed.
  - Applies to: Agent [Windows]
- Unapproved Publishers Missing in the Console [35282, 35295, 35316, 35319]
  - Details: After an upgrade from an earlier release, only approved publishers displayed in the Bit9 console. This release displays all publishers.
  - Applies to: Server
- Improvements in Console Performance [34944, 34974]
  - Details: This release eliminates several cases in which server operations could interfere with the performance of the Bit9 console.
  - Applies to: Server
- Write Block Custom Rules not Functioning Correctly [35125]
  - Details: When a Custom Rule was created that blocked writes to a file, a Notifier would appear indicating the write was blocked, but the file would be written anyway. This release allows Custom Rules to correctly block writes to files.

- Applies to: Agent [Mac]

- Network Files Incorrectly Identified as Local [34826]
  - Details: In some circumstances, files on the network would be incorrectly identified as local files. In this release, all network files are correctly identified as such.
  - Applies to: Agent [Mac]
- Updater Failing for Google Chrome on Mac [34839]
  - Details: When the Google Chrome updater was enabled, files from Chrome updates were still being blocked. In this release, the updater functions correctly and no files are blocked.
  - Applies to: Agent [Mac]
- Panic: "attempt to remove permanent VM map entry" [34995, 35031]
  - Details: In very rare circumstances, a system panic occurred immediately after installation of the Bit9 agent, especially when available memory was low. This release addresses the underlying issue that was causing the panic in these situations.
  - Applies to: Agent [Mac]
- Improved Access to Files on Remote CIFS and NFS File Systems [34404]
  - Details: Previous releases did not correctly impersonate the user identity used to access remote files that were mounted from */etc/fstab* using the CIFS and NFS file systems. This release allows access to these files.
  - Applies to: Agent [Linux]
- Missing Upgrade Package [34737]
  - Details: Certain releases of v7.0.1 did not include an installation package required for the upgrade of agents from prior versions of 7.0. This release includes the installation package.
  - Applies to: Server
- Pre-approvals not Present on Upgrade [34738]
  - Details: Certain releases of v7.0.1 did not include pre-approvals for the components of the Windows installation packages. This could cause blocks on endpoints that were attempting to upgrade. This release includes pre-approvals for all upgrade components.
  - Applies to: Agent [Windows], Server
- Improvements in the Notifier for Mac and Linux [35140]
  - Details: This release includes usability improvements to the Bit9 Notifier, including automatically scrolling to the top of notification text.
  - Applies to: Agent [Mac, Linux]
- New Supported Updaters for Mac [34697, 34729, 34731, 34788, 35090]
  - Details: Updaters for Google Drive, Adobe Reader, Adobe Flash, VMWare Fusion and Microsoft Office have been added to this release.
  - Applies to: Agent [Mac]
- Server Upgrade from v6.0 Fails when Server Debugging Enabled [35067, 35078]
  - Details: If the Bit9 server had debug logging enabled, upgrade from 6.0 to the current release would fail. This release allows an upgrade to proceed even if server debugging is enabled.
  - Applies to: Server

- Erroneous Schema Validation Errors on Upgrade [34853, 34913]
  - Details: On Bit9 servers that included saved Drift Reports, the upgrade process would sometimes report that the Bit9 schema was invalid. This release excludes certain Drift Report information from the upgrade schema validation process, allowing future upgrades to proceed without error.
  - Applies to: Server
- Agents with Large Numbers of Logged on Users Cannot Register [34811, 34856]
  - Details: The presence of a large number of logged on users, such as may occur on a terminal server, would prevent the Bit9 agent from properly registering with the server. This caused the agent to be unable to send events and to appear permanently offline. In this release, an agent with a large number of users is not prevented from registration.
  - Applies to: Agent [Windows]
- File Upload Failures [34668]
  - Details: Occasionally, file uploads to the Bit9 server would fail with an error in the server logs that mentioned *UpdateFileUpload*. In this release, the condition that caused these errors has been eliminated.
  - Applies to: Server
- Diagnostic Upload Fails with Non-default Server Port [34647, 35080]
  - Details: When the Bit9 server used a non-default communication port, this would prevent diagnostic file upload. In this release, diagnostic uploads function correctly, even with a non-default port.
  - Applies to: Server
- Events and Computers not Deleted as Requested [34686, 35028, 35089]
  - Details: In some circumstances, a background Bit9 server task that deleted events or computers would deadlock. This caused the associated items to remain, even after administrator-specified criteria had been met. This release resolves the underlying deadlock and allows events and computers to be deleted according to the administrator's specifications.
  - Applies to: Server
- Unable to Edit Policy Settings [35305]
  - Details: In rare circumstances, the Bit9 console would not allow Policies to be edited after a server upgrade. In this release, the underlying cause is corrected and Policy editing is always allowed.
  - Applies to: Server
- Health Check Improvements [34836, 34856]
  - Details: In previous releases, any health check failure, regardless of how serious, would show a red circle icon for the Connection Status of the relevant agent on the Computers table or Computer Details page. In this release, only the most serious health check issues will cause the Connection Status icon to show in red.
  - Applies to: Agent [Windows]
- 32-bit Registry Macros Yield Incorrect Data on Vista and Windows 2008 64-bit [34877, 35244]
  - Details: On 64-bit systems running Vista or Windows 2008, the 32-bit macros, such as *Reg:HKLM-SoftwareX86*, that are used in Custom Rules and elsewhere did not function correctly. In this release, all registry macros correctly retrieve the desired value.
  - Applies to: Agent [Windows]

- Addition of Office 2013 “Click to Run” Updater [33561]
  - Details: This release includes an updater that allows updates to Microsoft Office 2013 via Microsoft’s "Click to Run” streaming technology.
  - Applies to: Agent [Windows], Server
- Cannot Ban or Approve Files from an Approval Request [34779]
  - Details: In previous releases, it was not possible to approve or ban a file from an Approval Request. This release allows files to be approved or banned using a menu on the right of the console page.
  - Applies to: Server
- User Authorized for Approval Management Receives Error on Approval [34238, 34865]
  - Details: A user authorized to change the local state of a file could not do so from the link on the Approval Request Details page. Instead, they received an error “You are not authorized to modify the status of a file”. This release allows the local state of files to be changed from this page.
  - Applies to: Server
- Unable to Approve Devices with Ampersand in Serial Number [34685, 34720]
  - Details: If a device contained an ampersand (‘&’) character in its serial number, it could not be approved in the Bit9 console. In this release, such devices can be approved.
  - Applies to: Server
- “Ever Blocked” Column Empty in File Catalog [34679]
  - Details: In the File Catalog, the “Ever Blocked” column never showed a value. In this release, the column correctly displays “Yes” or “No.”
  - Applies to: Server
- Timeout in Events Threat Indicator View [34604, 34609, 34661, 34678, 34934]
  - Details: The Threat Indicator saved view for the Events page would time out when grouping resulting data. This release improves the performance of the Threat Indicator saved view.
  - Applies to: Server
- Bit9 Connector: Notifications not Pruned when Connector Disabled [34805]
  - Details: When any Bit9 Connector was disabled in the Bit9 console, any additional notifications received were never pruned. Since FireEye continues to generate notifications even when the Bit9 Connector is disabled, this could lead to excessive use of resources. In this release, pruning continues even when the Bit9 Connector is disabled.
  - Applies to: Server
- Bit9 Connector: Known Files Tab Shows All Files [34719]
  - Details: The “Known Files” tab in External Notification Details showed all files that were referenced in the associated notification, rather than just the new and modified files. This release correctly displays new and modified files only.
  - Applies to: Server
- Bit9 Connector: RBAC Improvements [34570, 34628, 34803]
  - Details: This release improves the mapping of RBAC permissions, which are set for Bit9 console login groups, to Bit9 Connector actions.
  - Applies to: Server
- Bit9 Connector: Palo Alto Networks WildFire Connectivity [34847, 34858]

- Details: When connectivity was lost to a Palo Alto Networks WildFire appliance, a server error event would be logged once per minute until connectivity was restored. In this release, the Bit9 server continues to contact the WildFire appliance for a limited time, after which the Connector is disabled and must be re-enabled manually. The default configuration allows an appliance to be down for approximately three and a half hours before the Connector is disabled.
- Applies to: Server

- Bit9 Connector: Issue Creating Report Only Ban from Event Rule [34919]
  - Details: When a Report Only Ban was created from an Event Rule, the ban would not appear on endpoints. In this release, the ban is sent to all appropriate endpoints.
  - Applies to: Server

Corrective Content in Parity 7.0.1 Release (Build 1364, Patch 7)

- Server Patcher Timeout [29423, 35129, 35130]
  - Details: In some circumstances, when the Bit9 database is large or its associated hardware is underpowered, the server patch installer would time out while applying changes to the Bit9 database. In this release, the patch installer allows as much time as needed for the changes to complete.
  - Applies to: Server
- File Blocked when Digital Signature Lacks Timestamp [34065, 34067]
  - Details: Files that were signed with a valid digital signature that lacked a timestamp would not be approved, even when the associated publisher was approved. This release considers all digital signatures as valid during the lifetime of the certificate, whether or not there is an associated timestamp.
  - Applies to: Agent [Windows]
- Unapproved Applications Executed from LaunchPad Hang System [26632, 34485]
  - Details: In Medium Enforcement, an unapproved application executed from the Launchpad would hang the system. The hang does not occur in this release.
  - Applies to: Agent [Mac]
- Agents Disconnected in Console until Restart [34254, 34350, 34351]
  - Details: In certain circumstances, agents would cease communicating with the Bit9 server and appear as offline, even though the agent was correctly enforcing its policy and TCP connectivity with the server was available. An agent restart would fix this issue. In this release, the communication problem is addressed.
  - Applies to: Agent [Windows], Server
- Health Check Improvements [34864]
  - Details: In previous releases, any health check failure, regardless of how serious, would show a red circle icon for the Connection Status of the relevant agent on the Computers table or Computer Details page. In this release, only the most serious health check issues will cause the Connection Status icon to show in red.
  - Applies to: Agent [Windows], Server
- Incorrect Health Check on Unapproved Module [34261, 34386]

  - Details: In some circumstances, an agent health check would report the presence of an unapproved module that did not actually exist on the agent (e.g. “C:\kernel32.dll”). This release corrects the underlying problem that allowed this to occur and ensures that the unapproved module health check only occurs when a genuinely unapproved module is loaded.
  - Applies to: Agent [Windows]
- Improvements to Active Directory Policy Switching [34217, 34482]
  - Details: In some circumstances, especially when certain types of VPN were in use, the Bit9 agent would not correctly switch Active Directory mapped policies based on user membership in Active Directory groups. This release provides mechanisms to force the agent to re-evaluate group membership. Please contact Bit9 Support if you need more information.
  - Applies to: Agent [Windows]
- Agent Crashes at Startup [34146, 34387, 34388, 34419]
  - Details: In rare circumstances, the Bit9 agent would crash at startup. These crashes are addressed in this release.
  - Applies to: Agent [Windows]
- Incorrect Escaping of “\” and “=” in CEF [34148, 34385]
  - Details: The CEF format for syslog output was incorrectly escaping the “\” and “=” characters, leading to missing data in ArcSight, which uses the CEF format. This release correctly escapes these characters.
  - Applies to: Server
- Updater Failing for Adobe Creative Suite [33687]
  - Details: The updater for the Adobe Creative Suite was failing, due to changes made by Adobe in the update process. This release adds an updater for Adobe Application Manager that covers the Adobe Creative Suite and allows updates to proceed correctly.
  - Applies to: Agent [Windows], Server
- Error Importing Certificate in Console [33974, 34470, 34599]
  - Details: Some attempts to import a certificate in the Console failed and produced an “Error Code 0.” This release allows certificates to be imported without error.
  - Applies to: Server
- Rule Test Page is Restricted [34180, 34260]
  - Details: The pages *TestRules* and *TestLogin* were unavailable to users authorized to manage login accounts and groups. This release correctly allows authorized users to access these pages.
  - Applies to: Server
- Improvements in Agent Re-synchronization [34538, 34619]
  - Details: In rare circumstances, explicitly re-synchronizing all file information on an agent would not reset certain internal information, leading to cases where resynchronization was incomplete. This release improves agent synchronization.
  - Applies to: Agent [Windows]
- High Server Backlog [29393, 32987]

    - Details: In some cases, the agent reported each file in a file group separately, when it should have been reporting them as a single group. In this release, files are grouped more efficiently, reducing the backlog on the server when there is high file volume.
    - Applies to: Agent [Windows]
- No Event for Uploaded File Deletion [34484]
    - Details: When files that were uploaded to the Bit9 server were deleted, no event for the deletion would be sent. This release sends an event when any uploaded file is deleted.
    - Applies to: Server
- Incorrect Restrictions on Certificate Validity Check [34361, 34517]
    - Details: In prior releases, the agent would check the validity of all certificates in a certificate chain. If any certificate in the chain was not within its validity period, then the leaf certificate would not be considered valid. In this release, the validity of the non-leaf certificates is not considered. Note that correct validity information may not show in the Console until the associated agent's file information is re-synchronized with the server.
    - Applies to: Agent [All]
- Upgrade Issues from 7.0.0 [34708, 34723, 34724]
    - Details: In previous 7.0.1 releases, upgrades from 7.0.0 agents were unsuccessful. This release allows upgrades from 7.0.0 to occur correctly and includes preapprovals for the associated patch file.
    - Applies to: Server
- Trusted User Unable to Run Unapproved Files [34382]
    - Details: In some circumstances, a Trusted User was unable to run unapproved files. This release corrects this issue.
    - Applies to: Agent [Windows]
- Improvements in Display of IP Addresses in Events [33997, 33998]
    - Details: In previous releases, the Events page displayed the *current* IP address of an agent associated with an event. In this release, events display the IP address at the time the event was reported.
    - Applies to: Server
- Files in the Recycle Bin are Fully Tracked [34123]
    - Details: In previous releases, files in the recycle bin were fully tracked in the same way as executable files in other locations. In this release, tracking of files in the recycle bin is limited to those which execute.
    - Applies to: Agent [Linux]
- Memory Leaks in the Kernel Component of the Bit9 Agent [34181]
    - Details: In previous releases, two small memory leaks occurred in the kernel component of the Bit9 agent. These leaks are addressed in this release.
    - Applies to: Agent [Mac]
- Improvements in Agent Security [34443]
    - Several security issues affecting the Bit9 agent were addressed in this release.
    - Applies to: Agent [Windows]
- Meters Added Before Associated File Are Not Counted [34133]

- Details: If you created a meter to monitor execution of a file before the file identified in the meter was present on any endpoint, the meter would never count executions of the file. In this release, meters count all executions of the file they monitor, regardless of when the file is first seen.
- Applies to: Agent [Mac, Linux]

- System Hangs When Using BitLocker Encrypted Removable Devices [34606]
  - Details: In some circumstances, inserting a BitLocker-encrypted removable device would hang the system. This was due to a kernel deadlock. This release ensures that this deadlock does not occur.
  - Applies to: Agent [Windows]

Corrective Content in Parity 7.0.1 Release (Build 1290, Patch 6)

- Performance Improvements in Network File Access [29527, 33237]
  - Details: In previous releases, the Bit9 agent accessed network files using its own credentials rather than those of the currently logged on user. This could lead to long delays in network file processing. In this release, the order in which the credentials are used for network files is reversed, which reduces the likelihood of such delays.
  - Applies to: Agent [Windows]
- Cannot Make Policy Changes or Add New Policies [33658, 33610, 33651]
  - Details: In some circumstances, adding a new policy or changing an existing policy would give an error in the Bit9 console. In this release, policies can be added and edited successfully.
  - Applies to: Server
- Agent Crash on Trusted Directory [33654, 33656]
  - Details: When a Trusted Directory was deleted or disabled, the associated agent would crash if there were existing files that remained to be processed. The crash is addressed in this release.
  - Applies to: Agent [Windows]
- Agents Update Slowly [33729, 33787, 33897, 34296]
  - Details: The Bit9 server throttles events and other information sent by agents, in order to avoid being overloaded. In certain circumstances, this throttling would be too aggressive, preventing events from being uploaded and also preventing agent updates. This would delay the distribution of approvals and other policy changes to agents. In this release, the Bit9 server both throttles events less aggressively and provides additional configuration options for Bit9 Support to control this throttling. The agent performs additional validation of throttling data sent from the server.
  - Applies to: Agent [Windows], Server
- User-Based Active Directory Policy Mappings not Taking Effect [33663, 33949]
  - Details: In certain circumstances, Active Directory policy mappings based on the logged in user would not take effect in a reasonable time. This release ensures timely server processing of policy mapping information sent by the Bit9 agent.
  - Applies to: Agent [Windows], Server
- Files Discovered by Cache Consistency Check are not Correctly Processed in a Trusted Directory [33134, 33156, 33190]

  - Details: When a Cache Consistency Check discovered files in a Trusted Directory, the newly discovered files would not be properly trusted. This release ensures that newly discovered files are correctly handled by the Trusted Directory and are globally approved.
  - Applies to: Agent [Windows]
- Performance Improvements for File Delete and Rename [33072, 33990]
  - Details: When large numbers of files were deleted or renamed, the Bit9 agent on Mac would show greatly reduced performance or would temporarily freeze. In this release, the performance of deletion and renaming is improved.
  - Applies to: Agent [Mac]
- Notifier Displays UTF-8 Characters Incorrectly [26615]
  - Details: File names containing UTF-8 characters (e.g. "é") beyond the ASCII range would not correctly display in the Notifier. This release correctly displays Notifier text containing such characters.
  - Applies to: Agent [Mac]
- Expanding Groups of Items in Tables Causes 500 Error [28683, 28987]
  - Details: In some circumstances, expanding large groups of items in tables (e.g. files grouped by hash) would cause a browser error 500 in the Console. This release allows large numbers of groups to be expanded without an error.
  - Applies to: Server
- Improvements in Console Security [33192, 33193, 33227, 33249, 33353, 33470]
  - Details: Several security issues affecting the security of the Parity console were addressed in this release.
  - Applies to: Server
- Local Approvals Cannot be Removed [33352]
  - Details: When all files on a system were transitioned to Locally Approved via the "Change Local State" menu on the Computer Details page, the approval of individual files could no longer be removed. This release allows individual files to be transitioned to Unapproved in this circumstance.
  - Applies to: Agent [Mac, Linux]
- Events Received for Excluded Processes in File Integrity Rules [33347, 33356]
  - Details: Processes that were explicitly excluded from File Integrity Rules would still generate events. In this release, exclusions are properly applied and no events are generated.
  - Applies to: Agent [Mac]
- Agent Crash Processing ZIP File in Trusted Directory [33138, 33150, 33154]
  - Details: ZIP files larger than 4GB or containing more than 65,535 entries would cause the agent to crash when processing a Trusted Directory. This release handles large ZIP files correctly.
  - Applies to: Agent [Windows]
- Agent Crash Capturing Diagnostics [33139, 33150, 33155]
  - Details: In rare circumstances, capturing diagnostics would cause the agent to crash. This release allows diagnostics to be collected.
  - Applies to: Agent [Windows]
- Problem Processing LZMA-encoded Files in Trusted Directory [34223, 34326]

  - Details: Certain types of LZMA-encoded files in a Trusted Directory would not be correctly processed, leaving some files that should have been approved in an unapproved state. This release corrects the issue.
  - Applies to: Agent [Windows]
- Files in the Recycle Bin are Fully Tracked [33241]
  - Details: In previous releases, files in the recycle bin were fully tracked in the same way as executable files in other locations. In this release, tracking of files in the recycle bin is limited to those which execute.
  - Applies to: Agent [Mac]
- Incorrect Paths Reported in Events for Files in "/proc" [33414]
  - Details: A file named "/proc/file" in the "/proc" special file system would appear in events incorrectly as "/proc/proc/file". This release corrects this repetition.
  - Applies to: Agent [Linux]
- Justification Request Causes Notifier to Block the File [33593]
  - Details: In Medium Enforcement, submitting a justification request would automatically block the associated file. In this release, the Notifier remains open to allow the user to select their preferred action.
  - Applies to: Agent [Mac, Linux]
- Execution Control Custom Rule not Enforced [33607]
  - Details: When an Execution Control Custom Rule blocked a process that was run from the shell, use of the "-c" shell argument could cause the rule not to be enforced. In this release, the execution is properly tracked and blocked.
  - Applies to: Agent [Mac]
- Enabling a Script Rule with Rescan Approves Unrelated Files [34011]
  - Details: When a script rule was enabled with the rescan option, all unapproved files on the affected systems would be approved. In this release, only the script files matching the rule are approved and other unapproved files remain unaffected.
  - Applies to: Agent [Mac, Linux]
- New File Discovery Event does not Appear [29447]
  - Details: In rare circumstances, the "computer discovered new file" event was not displayed when a new file was run and blocked, although in these cases the "Execution block" and "New file on network" events were correctly displayed. This release correctly displays all three events.
  - Applies to: Server
- Error when Refreshing Meter Report Page [33594]
  - Details: When the time range for a Meter Report was set to "In the past," refreshing the page gave an error. In this release, the error no longer occurs.
  - Applies to: Server
- Agent Upgrade Fails to Upgrade Driver [33755]
  - Details: In rare circumstances, the agent upgrade process would not correctly upgrade the Bit9 driver, leading to upgrade failures. This release improves the driver upgrade process to allow the upgrade to succeed.
  - Applies to: Agent [Windows]
- Certificates Incorrectly Identified as Expired [34206]

- Details: When validating whether a certificate was expired, the expiration times of parent certificates was incorrectly considered. In this release, a certificate is considered valid if it was issued within the expiration period of its parent certificates, whether those parents are currently expired or not.
- Applies to: Agent [Windows]

Corrective Content in Parity 7.0.1 Release (Build 1164, Patch 5)

- Health Check Failure: "signed but did not pass file validation" [33685]
  - Details: In certain previous releases, all Bit9 agents would indicate a health check failure that "parity.exe is signed but did not pass file validation" with an associated error code of 80096005. This would cause the "Connection Status" for all agents on the Computers page to show a red circle, and the details page for each computer to indicate "Failure" in the "Health Check" field. In this release, these erroneous health checks are no longer reported.
  - Applies to: Agent [Windows]
- Issues Undocking Laptops [29541, 29982]
  - Details: In some circumstances, the Bit9 agent would prevent a laptop from undocking gracefully. In such cases, the error message "The service parity vetoed a hardware profile change request" would appear in the Windows Event log. This release corrects this issue and allows the undock to proceed without an error.
  - Applies to: Agent [Windows]
- Mac Becomes Unresponsive During Initialization [29802, 33094]
  - Details: During agent initialization, some Mac systems would become unresponsive. Once initialization was complete, the systems would respond again. This issue was caused by an interaction with Bootcamp. In this release, interactions with Bootcamp are correctly handled and systems are responsive during initialization.
  - Applies to: Agent [Mac] , Server
- Certificate Validation Fails Due to Common Name Mismatch [29220, 33146]
  - Details: Agents connecting to the Bit9 server validate the certificate of the server to which they are connecting. In some circumstances, this validation would fail due to a Common Name (CN) mismatch. This release allows the checking of the Common Name to be disabled when this is required.
  - Applies to: Agent [Windows]
- Active Directory Policy Mappings not Effective for Mac Platform [33073, 33157]
  - Details: Bit9 Active Directory (AD) policy mapping rules were not affecting agents on AD-managed Mac systems. This release allows Mac agents to be correctly assigned to a policy based on their Active Directory group membership.
  - Applies to: Agent [Mac]
- High Server Backlog [29393, 33171]
  - Details: In some circumstances, where the volume of new files on endpoints was large, the Bit9 server would develop a large backlog processing the reported information for "Files on Computers." This release improves the performance of the handling of files reported by agents, thus avoiding the backlog and keeping "Files on Computers" information more current.
  - Applies to: Server

- Server Patcher Timeout [29644]
  - Details: In some circumstances, the patch installer for the Bit9 server would time out while applying changes to the Bit9 database. This release waits indefinitely for database changes to be applied.
  - Applies to: Server
- Global Approval Action Clears Filters on Find Files Page [29462, 29534]
  - Details: On the "Find Files" page in the Bit9 Console, selecting files and globally approving them from the "Action" menu would reset the filters that determine which files appear on the page. In this release, the filters remain in place.
  - Applies to: Server
- Cannot Select Blocked Files for Approval from Event List [29387, 29426]
  - Details: Previously, blocked file events that did not include the file name could not be selected (checked), which prevented approval of the file from its event. In this release, any blocked file event that shows an associated file hash may be selected, allowing approval directly from the events page.
  - Applies to: Server
- Incorrect Copyright Date in Bit9 Console [29830, 32616]
  - Details: The Bit9 Console displayed an incorrect date in its copyright message. This release displays the correct date.
  - Applies to: Server
- No Results when Filtering Files by Detached Publisher [33169]
  - Details: In some circumstances, filtering a table of file instances by detached publisher would return no results, even when there were files that matched the filter. In this release, filtering by detached publisher returns the correct result set.
  - Applies to: Server
- Files Discovered by Cache Consistency Check are not Correctly Processed in a Trusted Directory [33156, 33190]
  - Details: When a Cache Consistency Check discovered files in a Trusted Directory, these newly discovered files would not be properly trusted. This release ensures that newly discovered files are correctly handled by the Trusted Directory and are globally approved.
  - Applies to: Agent [Windows]
- Active Directory Security Domain Configuration Does Not Support Multiple Domains [33002, 33213]
  - Details: In past releases, only one Active Directory Domain could be specified in the "AD Security Domain" setting on the General tab of the System Configuration page. In this release, multiple Domains may be supplied by separating them with semi colons.
  - Applies to: Server
- Improvements to Windows Update Support [33189]
  - Details: In some circumstances, some files from certain Windows Updates would be blocked. This release improves the agent's handling of the Windows Update process to allow these files to be correctly approved.
  - Applies to: Agent [Windows]
- Improvements in Console Security [29653, 29688, 33161, 33178]
  - Details: Several security issues affecting the security of the Parity console were addressed in this release.

    - Applies to: Server
- Issues Upgrading Agents from HotFix [33158, 33165]
    - Details: With certain HotFix agent versions installed, the Bit9 server did not schedule agent upgrades. This release correctly upgrades all appropriate HotFixed agents to the latest patch version.
    - Applies to: Server
- Server Upgrade Failing on SQL Server 2005 [33108, 33234, 33361]
    - Details: Bit9 installations that were using SQL Server 2005 would fail to correctly upgrade to the latest version. This release correctly upgrades Bit9 installations that use this SQL Server version.
    - Applies to: Server
- Server Upgrade Failure from Earlier Versions of 7.0.1 [29646, 29299]
    - Details: In some circumstances, upgrades from earlier versions of 7.0.1 would fail when manual changes had been made in the Bit9 database schema. This release corrects an underlying issue that prevented the installer from detecting schema modification, and will abort the upgrade process if such changes are detected.
    - Applies to: Server
- Console Timeout Error after Upgrade from 7.0.0 [29747, 29825]
    - Details: After an upgrade from Bit9 7.0.0, the Bit9 Console would timeout when accessing many pages. This release corrects the underlying cause of the timeouts and allows the Bit9 Console to function correctly.
    - Applies to: Server
- Changing Preferences in the Bit9 Console does not Confirm Changes [29894, 29964]
    - Details: When changes were made on the console Tools/Preferences page, clicking “Save” on that page returned to the previous page in the console history without confirming that the preference changes were saved. In this release, a confirmation message is displayed when “Save” is clicked on the Preferences page, and the console remains on that page.
    - Applies to: Server
- Improvements in Trusted Directory Scanning Performance and Diagnostics [20338, 29369, 29535, 29651]
    - Details: This release includes many improvements to Trusted Directory performance and diagnostics, including the ability to control whether certificates are validated on Trusted Directory content and the time that the agent pauses between processing each file in a Trusted Directory.
    - Applies to: Agent [Windows]
- Performance Improvements in Configlist Updates [32619, 33163]
    - Details: In some circumstances, having a large number of globally approved files caused slow updates to the configlist of agents running in Visibility mode. This release improves the performance of configlist updates in this case.
    - Applies to: Agent [Windows]
- Periodic Maintenance on Agent Cache [29884, 29940, 30002, 30006]
    - Details: In this release, periodic maintenance on the agent’s cache (*cache.db*) has been improved, including releasing any unused disk space.
    - Applies to: Agent [Windows]

- Improvements to the Firefox Updater [29978]
  - Details: This release includes improvements to the Mozilla Firefox updater to account for changes in the underlying update process. Note that these changes do not retroactively approve any files that were previously blocking.
  - Applies to: Agent [Windows]
- Improvements to the Google Chrome Updater [27420]
  - Details: This release includes improvements to the Google Chrome updater to account for changes in the underlying update process. Note that these changes do not retroactively approve any files that were previously blocking.
  - Applies to: Agent [Windows]
- Agent Upgrade Failed to Execute [26651, 26694]
  - Details: When asked to upgrade from earlier releases, agents were attempting to write upgrade log files into a location protected by Bit9 tamper protection. This would cause the upgrade to fail. In this release, agents are instructed to use a location for the log files that is not protected.
  - Applies to: Server
- "Days Offline" Column Blank on Computers Page [29413]
  - Details: In some circumstances, the "Days Offline" column on the "Computers" page in the console would be blank for offline systems. In this release, offline systems correctly display the amount of time they have been offline.
  - Applies to: Server
- Resetting Preference Settings does not Work [33058]
  - Details: Resetting the preference settings on the console Tools/Preferences page would not reset all display settings. For example, the number of items displayed would remain at its previous value and not revert to the default of 25. In this release, all preference settings are properly reset.
  - Applies to: Server
- Extraneous Text in Events that Contain Extended Characters [29235]
  - Details: When displaying events containing UTF-8 characters (e.g. "é") beyond the ASCII range, the event text would contain extraneous characters. This release correctly displays events containing such characters.
  - Applies to: Server
- No Confirmation Before Global Ban of Files [33055]
  - Details: In previous releases, choosing "Ban Globally" for a list of files on the "Find Files" page banned the files immediately, without requiring confirmation. In this release, users must respond to a confirmation dialog to ban the files.
  - Applies to: Server
- Error Displaying Drift Report Details [29659]
  - Details: Selecting "View Details" on a drift report would result in an error in the Bit9 console. This release allows drift report details to be viewed.
  - Applies to: Server

- No Event for Execution Allowed for Trusted User [25813]
  - Details: With an agent in High or Medium Enforcement, no event was displayed in the Bit9 console for execution of an unapproved file by a Trusted User. In this release, an execution allowed event, "Execution allowed (trusted user)", is displayed.
  - Applies to: Server
- Certain RSS Portlets Display Stale Content [25716]
  - Details: Some portlets in the Bit9 console dashboard were displaying out-of-date information. This release updates the associated RSS feeds to ensure that up-to-date news and information is displayed.
  - Applies to: Server
- Certain Trusted Directory Content not Approved [26731]
  - Details: In some circumstances, certain Microsoft Installer files would not be properly approved when added to a Trusted Directory. This release addresses this issue, ensuring that all Trusted Directory content is properly approved.
  - Applies to: Agent [Windows]
- Configlist Version on Server Less than on Agents [29571]
  - Details: In rare circumstances, the Bit9 server would fail to increment its configlist version, leading agents to have a configlist version that was higher than the server. Because of this, the agents would not update their configlist when appropriate. In this release, the underlying error condition is correctly handled and the server correctly increments its configlist version.
  - Applies to: Server
- Improvements in Installation Package Generation [33089]
  - Details: Occasionally, previous error conditions encountered while generating agent installation packages would prevent the Bit9 server from regenerating them in the future. This release improves the generation process to recover from such error conditions more effectively.
  - Applies to: Server
- Improvements in Agent Cache Efficiency on Trusted Directories [33123]
  - Details: In this release, changes have been made to the retention of historical events in the agent cache (*cache.db*), which primarily affect systems that implement Trusted Directories. This change reduces the size of the cache and improves processing efficiency, especially on large Trusted Directories.
  - Applies to: Agent [Windows]
- Agent Crash on Shutdown [33167, 34226]
  - Details: On Mac systems, the Bit9 agent would crash when shutting down. In this release, the agent shuts down cleanly.
  - Applies to: Agent [Mac]
- Agent Crash during Initialization [33445]
  - Details: In some circumstances, the Bit9 agent on Linux systems would crash during initialization. This release corrects the underlying issue so that agents initialize successfully.
  - Applies to: Agent [Linux]

- Linux System Locks Up under Heavy Load [29417]
  - Details: Under heavy load, Linux systems would occasionally lock up for a few seconds before continuing normal operation. In this release, such lockups no longer occur.
  - Applies to: Agent [Linux]
- Tamper Protect During Mac Agent Upgrade [29936]
  - Details: During Mac agent upgrades, tamper protection events would be received for the upgrade log file. The log file would subsequently contain no data. In this release, the upgrade log is successfully generated and no tamper protection events occur.
  - Applies to: Agent [Mac]

Corrective Content in Parity 7.0.1 Release (Build 1109, Patch 4)

- Improvements in Offline Certificate Validation [33098, 33111]
  - Details: In previous releases, when certificates could not be successfully validated, for example on permanently offline systems, a fallback approach checked an internal revocation list. In some circumstances, this list was applied incorrectly. In this release, the certificates on this internal list are correctly handled.
  - Applies to: Agent [Windows]
- Agent Upgrade Issue [29756]
  - Details: In prior releases of Parity 7.0.1, upgrading an agent would cause corruption issues with its local cache database. This release correctly upgrades prior releases and also remediates any database corruption, while preserving all data.
  - Applies to: Agent [Windows]

Corrective Content in Parity 7.0.1 Release (Build 1096, Patch 3)

- Enhancements in Digital Certificate Processing [29483]
  - The digital certificate used to sign prior releases has been revoked. In addition to using a newly issued certificate, this release will explicitly unapprove any software that was previously signed by the revoked certificate, even when "Bit9" is a Trusted Publisher. This prevents any software signed by this certificate from running in Medium or High Enforcement.
  - Applies to: Agent [All]
- Support for Hard Links on Mac and Linux Platforms [28627, 28634]
  - Details: Hard links are now supported on Mac and Linux platforms.
  - Applies to: Agent [Mac, Linux]
- Additional Fixes
  - Details: This release contains many additional fixes for both customer-reported and internally discovered issues.

Corrective Content in Parity 7.0.1 Release (Build 860, Patch 2)

- Parity Agents not Connecting to Parity Server [27482]
  - Details: In some environments, Parity agents would not connect to the Parity server, and the server would log errors for *AcceptSecurityContext*, referencing error code 0x80080321. This error indicated a failure to properly negotiate the SSL connection between agents and the server. This release corrects the underlying issue with SSL negotiation in the Parity Server.
  - Applies to: Server

- Stop Error 0x000000DF on Windows 2003 Server [28566]
  - Details: On Windows 2003 Server systems, a Stop Error with the code 0x000000DF (*IMPERSONATING_WORKER_THREAD*) would occur in certain circumstances. This release ensures that the Parity driver correctly manages internal system resources in a way that is compatible with older versions of Windows and that works correctly in conjunction with Symantec Antivirus.
  - Applies to: Agent [Windows]
- Hang When USB Storage Device Inserted [28560]
  - Details: On systems where Symantec Anti-virus is installed, the system may hang when a USB storage device is inserted. The Parity driver was waiting for information from the system that was not yet available on initial insertion of the USB device. This release does not wait for this information.
  - Applies to: Agent [Windows]
- Initialization Fails to Identify All Pre-existing Files [28564]
  - Details: When an agent received a request for a cache consistency check during initialization, the initialization process would be incorrectly terminated. This would later cause pre-existing files to block when in High Enforcement. In this release, cache consistency checks are ignored until initialization is complete.
  - Applies to: Agent [Windows]
- Limited Support for Hard Links on Mac and Linux Platforms [28627, 28634]
  - Details: In this release, Parity does not track or report files hard-linked to other files. An example of this occurs when using the Mac Finder to drag an application between folders. This issue will be addressed in the next Parity patch release.
  - Applies to: Agent [Mac, Linux]
- Mac OS X 10.8 Kernel Panic After Software Update [28635]
  - Details: Previously, if a Software Update was applied during agent initialization, a kernel panic would occur when the system was subsequently rebooted. This release improves support for Software Update and prevents the panic.
  - Applies to: Agent [Mac]
- Mac Kernel Panic on Block of *xpchelper* from Software Update [28636]
  - Details: On systems in High Enforcement with automatic updates enabled, a Parity block on *xpchelper* would cause a kernel panic. This release improves support for Software Update to prevent the block and subsequent kernel panic.
  - Applies to: Agent [Mac]
- Console Does Not Display Full Path for Process in Events [28639]
  - Details: For Mac and Linux agents, the Parity console did not display the full path for processes on the Events page. In this release, the full process path is displayed.
  - Applies to: Agent [Mac, Linux]
- Agent Reboot During Initialization Resets Initialization Percentage to Zero [28641]
  - Details: On Mac and Linux platforms, a reboot during initialization would reset the percentage to zero and would not correctly resume initialization. This release resumes initialization at the correct point after a reboot.
  - Applies to: Agent [Mac, Linux]

- Linux Installer Fails When *unzip* is not Present [28670]
  - Details: The Linux agent installer would fail when the *unzip* program was not present on a system. This release checks for the presence of *unzip* and warns that it must be installed before the Parity installation can continue.
  - Applies to: Agent [Linux]
- Improvements to Windows Update Support [28682]
  - Details: In some circumstances, certain Windows Updates would result in blocks of files. This release improves the agent's handling of the Windows Update process to allow these files to be correctly approved.
  - Applies to: Agent [Windows]
- Parity Agents Constantly Out of Date [28539]
  - Details: In some circumstances, the Parity server would not correctly propagate approvals and rules to agents. This occurred when certain types of Custom Rules were to be sent. In this release, the server correctly sends these rules, allowing agents to update.
  - Applies to: Server
- Performance Issues with Network Files [28577]
  - Details: When accessing files over a network, the Parity agent would cause a marked slowdown in the performance of certain operations, such as copying files. By caching additional internal information, this release improves the performance of operations on network files.
  - Applies to: Agent [Windows]
- Agent Reinitializing After Database Corruption [28581]
  - Details: In some circumstances, a hard reset, power failure or system crash can corrupt the Parity agent's database. If this occurred more than once within a 12-hour period, the agent would reinitialize and need to download information from the Parity server, which could lead to unexpected agent behavior, including blocks. In this release, the agent is more resilient to the failures that caused this condition.
  - Applies to: Agent [Windows]
- Excessive Agent Log Files [28567]
  - Details: In previous releases, the Parity agent would not correctly clean and rotate its log files. This release adjusts log rotation to account for both the total number of files and their overall size, reducing the space consumed.
  - Applies to: Agent [Windows]
- Health Check Fails on Windows 2008 R2 Server Core [28546]
  - Details: On systems running Windows 2008 R2 Server Code, the built-in Parity health check mechanism would incorrectly check the certificate on a Windows system file that does not exist on Server Core, producing an erroneous health check failure. For this release, the health check is performed using a Windows system file that exists on all Windows platforms.
  - Applies to: Agent [Windows]
- Agents Show "Reboot Required" After Reboot [28587]
  - Details: In some circumstances, when Parity was newly installed on Windows 2003 Server or Windows XP, the "Reboot required" status would not be cleared, even after a reboot. In this release, the status is correctly cleared.
  - Applies to: Agent [Windows]

- Agents Fail to Upgrade Until User Logon [28591]
  - Details: If an agent was moved from a Policy that did not allow upgrades into a Policy which did, it would fail to upgrade until a user logon caused the agent to re-register with the server. During this time, the agent would remain in "Not requested" state in the Parity console. In this release, the server correctly flags an agent for upgrade when it is moved into a Policy that has upgrades enabled.
  - Applies to: Agent [Windows]
- Excessive Network Traffic from Parity Agent After Upgrade [28536]
  - Details: After an upgrade, the Parity agent was reporting information to the Parity server on all approved and banned files, causing an increase in network traffic. In this release, only changes in the state of the files are reported to the server.
  - Applies to: Agent [Windows]
- Agents Erroneously Moving Between Enforcement Levels [28562]
  - Details: For Policies assigned by Active Directory mapping, agents would occasionally move between Enforcement levels unexpectedly. This release corrects issues in the mapping mechanism.
  - Applies to: Server
- Changing Time Zone Does Not Affect Event Timestamps [28557]
  - Details: When the Parity server time zone was changed in the System Configuration section of the Parity console, the timestamps of events displayed by the console was incorrect. In this release, the timestamps correctly display in the chosen time zone.
  - Applies to: Server
- Parity Console Fatal Error [28545, 28555]
  - Details: When many agents in a large deployment were initializing, the Parity console would occasionally give a fatal error. This required the Parity server to be restarted to regain access. This release resolves the error.
  - Applies to: Server
- Alerts Not Triggering Correctly [28569]
  - Details: An internal Parity server task that tracks data for alerting was not functioning correctly, which caused alerts not to be correctly triggered. In this release, the internal task is corrected and alerts now trigger correctly.
  - Applies to: Server
- Filters Reset on Find Files [28578]
  - Details: In the Parity console, the Find Files page would incorrectly reset filters when moving to and from the page. This release correctly retains any filters in this case.
  - Applies to: Server
- Database Backup Fails After Upgrade [28547]
  - Details: After an upgrade from Parity version 6, backups were no longer being made. In this release, database backups correctly function after an upgrade.
  - Applies to: Server

Corrective Content in Parity 7.0.1 Release (Build 806, Patch 1)

- Mapping policies based on domain membership not supported on Linux [25632]
  - Details: Linux agents did not display fully qualified domain names, so mapping to policies using Active Directory rules based on domain membership was not supported on Linux clients. This release now supports this functionality.
  - Applies to: Agent [Linux]
- Notifier only loads for the user that performed the agent installation [26151]
  - Details: On OS X, the Parity Notifier would not load at startup for some users in multi-user environments. In this release, the Parity Notifier will load at startup for all users in multi-user environments.
  - Applies to: Agent [Mac]
- Trusted groups not fully supported on Linux clients [26374]
  - Details: On Linux clients, a user with the same name as a trusted group would not be recognized as trusted in Parity. This release removes that restriction.
  - Applies to: Agent [Linux]
- Parity Server error when capturing statistics [26827]
  - Details: In previous releases, a permission issue caused the Parity Server to log a misleading message. This permission issue has been eliminated so that the Parity Server can correctly communicate statistics to the log files.
  - Applies to: Server
- Automatically downloaded updates get blocked [26848]
  - Details: When automatic downloads are enabled for Software Update on Mac OS X, the automatically downloaded installer packages are not approved in Parity. Because of this, when Software Update later attempted to install these packages, they would be blocked by Parity Agents in High Enforcement policies. In this release, the trusted updater rules have been enhanced to avoid this problem.
  - Applies to: Agent [Mac]
- Installation does not work with full path [26863]
  - Details: When running a Linux agent installation package, you previously needed to be in the same directory as the package or you would receive an error message and the installation would fail. For example, if you download a package called high-enforcement-redhat6.bsx to /home/user/downloads you needed to change to that directory before executing the script. In this release, you can run a Linux installation package from any directory by specifying the full path to the script.
  - Applies to: Agent [Linux]
- Pressing 'E' to exit Patcher doesn't exit [26901]
  - Details: If an error occurs during patch installation, the user is presented with the option to continue or to exit. If the user entered 'E' to exit, the installation would continue anyway. In this release, the script will now properly exit.
  - Applies to: Server
- Mac agent doesn't finish sync [26925]
  - Details: Multi-byte characters in file names could cause the agent not to synchronize file information. This release properly handles files with multi-byte characters in their names.
  - Applies to: Agent [Mac]

- Agents unable to upgrade from 7.0.1.475 [26925]
  - Details: The 7.0.1.475 Parity Agent was being identified as a non-upgradable beta version. In this release, the 7.0.1.475 Parity Agent is correctly identified as being upgradable.
  - Applies to: Agent [Windows, Linux, Mac]
- "Incorrect Syntax" error in Parity Console [27079]
  - Details: In some circumstances, the Parity Console Dashboard would display an "Incorrect Syntax" error after a user logged into the console. This has been addressed in this release.
  - Applies to: Server
- Agents are not connecting to the server [27483]
  - Details: In some circumstances, Parity Server would fail to negotiate an SSL connection with agents due to a buffer size limitation. In this release, the buffer size has been increased to resolve this issue.
  - Applies to: Server

Enhancements and Improvements

- Alerts now include a list of computers that have potential risks.
- Improved bulk activities, such as importing bulk approvals.
- Improved protection of Parity and its data on agents.
- Many installer improvements, especially on error conditions.

Known Issues and Limitations

- Users should not rename the connector MSI file when installing the Bit9 Connector. Otherwise, in future releases, upgrades may be prevented. [41865]

- When you enable or create a new script rule, agents that are still initializing do not stop and restart their initialization. Because of this, files that match the script rule but are in directories that have already been scanned will not be discovered and added to the Bit9 file inventory. [37026,37056]

  To make sure that all appropriate files are discovered in this situation:
  1. Go to the Computer Details page for the computers that were still initializing.
  2. In Advanced menu, choose **Perform Cache Consistency Check > Full Scan for New Files**.

  Another alternative, if you want to approve all files matching this script rule, would be to disable the rule, check the **Rescan Computers** box, and then save and re-enable the rule. This will discover and approve all files matching this script on connected machines that are not in initialization.

  Note: To avoid this issue, Bit9 recommends configuring all script rules prior to deploying agents.

- 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]

- On Apple Mac OS 10.9 or later the b9kernel.kext file is installed in /Library/Extensions instead of /System/Library/Extensions. Keep this in mind when configuring anti-virus scanning exclusions.

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

- When you submit a file to a FireEye target folder for analysis, the Status column on the Requested Files page Analyzed Files tab might show multiple results for the single analysis (e.g., Analyzed (1,2,3)). In this case, only the number representing the actual analysis environment is a working link to the External Notification Details for the results. [36800]

- 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 Parity 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 Parity 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 Parity 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 both the Bit9 agent and Microsoft Enhanced Mitigation Experience Toolkit (EMET) are installed on a Windows system, there can be interaction issues between the two, including disabling of Bit9 bans. To avoid these issues, either work with the EMET to exclude Bit9 files from being managed, or Install Bit9 prior to installing EMET.

- If you use the "Export to CSV File" feature in a Parity 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 Parity 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.

- In Memory Rules: Do not use Prompt as the action for Dynamic Code Execution rules. This could cause a deadlock situation.

- If a Registry Rule is configured to block writing to a full path (no wildcard on the left), the rule will block attempts to rename and delete a key or value, but it will not block creation of a new key. However, no values can be created under this key.

- By default, computers running Microsoft Vista or Windows 7 operating systems have User Access Control (UAC) enabled. With UAC, users are not actually members of a built-in, privileged group unless they have been given "elevated privilege". Because of this, a Parity rule that relies on a pre-defined group to identify a user may not work for computers running Vista or Windows 7. If a group

definition is necessary for a rule, consider using security groups you have defined rather than the pre-defined groups.

- On Mac OS X, an interoperability issue exists with certain versions of Trend Micro's endpoint security products. Be sure to upgrade to the latest version of these Trend Micro products before installing Parity agents. [26565]

- On systems running OS X 10.6.8 and earlier, some system processes attempt to make directory modifications that violate Bit9 Tamper Protection rules, and this will trigger Tamper Protection events on the server. In OS X 10.7 and later, this system process behavior was removed, and these Tamper Protection events will not be seen.

- Parity uses the actual user context of a process when applying user-specific rules or approval by a trusted user. When the effective user differs from the actual user (such as it is when *sudo* is used), Parity still identifies the actual process user, and will not use the effective user when attempting to match a rule. For example, a Parity rule that allows *root* to run a process to access a file will not allow that process to access the file if it is run via *sudo*. [25217]

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

  Software Updates blocked by the SEP/Parity interaction produce two events in the Parity 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. [29117, 33147]

- Changes in Parity 7.0.1 require that the collation of the Parity Server database be set to the default US English collation. If the collation is set to something different, you will not be able to upgrade to 7.0.1, and you will be alerted that you need to contact Bit9 Support for assistance with the upgrade. [27119]

- When upgrading Parity 7.0.1 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. Parity upgrade will continue when this step is complete. [29819, 29822]

- When a Notifier appears on an agent, if the Notifier Link field contains a "mailto" address, and the target application for sending mail is not DEP compatible, the application may not launch when the link is selected, even if the associated mail 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 Windows after installing the agent is not supported, and doing so will produce health check failures and in some cases failure of the Windows upgrade. If you need to upgrade Windows or you see a health check failure that reports a mismatch between the agent and the build platform, contact Bit9 Technical Support for remediation recommendations. Service pack upgrades are fully supported and do not cause health check failures. [33646]

- For Mac, 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]

- When using Internet Explorer 11 to run the Bit9 Security Platform server, the warning message stating IE11 is not supported can be ignored.

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 (Parity Server, Parity Agent, or Parity Knowledge) and version number
Hardware configuration	Hardware configuration of the Parity 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