10 December 2018 Release Notes

Private Cloud Administration Portal 3.0.2

Bugfixes/Enhancements
• Fixed an issue where error logs were not handled correctly during a restore from backup.

16 November 2018 Release Notes

Private Cloud Administration Portal 3.0.1

New
• In Private Cloud 3.0.1, Airgap Mode has been deprecated; however, existing customers with Airgap Mode will be grandfathered in.

IMPORTANT! To upgrade to Private Cloud 3.0.1 you must do a Backup/Restore from a 2.4.0 or newer device, and have Disposition Server Extended Protocol enabled, which may require several system migrations. Users performing a Backup/Restore from a 2.4.x device will be exempt from the Trusted Certificate requirement during install. Any new services (such as the Authentication) will be subject to the new mandatory hostname requirements. Users will have to set valid hostnames and upload a cert/key pair for all new services during the initial install wizard.
16 November 2018 Release Notes

- Hostnames and a certificate/key pair are now required for all services:
  - Administration Portal
  - Authentication (new in Private Cloud 3.0.1)
  - FireAMP Console
  - Disposition Server
  - Disposition Server - Extended Protocol
  - Disposition Update Service
  - Firepower Management Center
- Users can upload the root certificate for custom Certificate Authorities during the initial install wizard.
- Wildcard certificates are permitted.

Bugfixes/Enhancements
- There is no longer a distinction between manual and scheduled backups. This means that both kind of backups are subject to the same retention policy.
- We no longer allow backups to fill the disk. As backups can become very large, we perform a check and do not allow backups to be done if they will fill a disk above 90%. We will also remove the oldest backups if required.
- We do not allow multiple backups to be triggered at the same time.
- We do not allow a backup to be performed on an Airgapped device if a ProtectDB import is running.
- A new license type has been added. This is to support the hardware device, but can be used on a virtual appliance.

FireAMP Console 5.3.20180910

New
- Add “Upload Successful” message when uploading endpoint IOC.

Bugfixes/Enhancements
- Fixed a problem with portal file_repository page breaking when one of the fetched file checksum is in an application control blocking list.
- Allow OOXML_* files to be cloud queried.
- CVEs are now limited to 45 per event.
- CVEs are now emitted weekly, instead of daily.

AMP for Endpoints Windows Connector 6.1.7

Bugfixes/Enhancements
- Fixes for multiple ClamAV vulnerabilities:
  - CVE-2018-0360
16 November 2018 Release Notes

- CVE-2018-0361

**IMPORTANT!** Malicious Activity Protection and Exploit Prevention are not yet supported in Private Cloud.

AMP for Endpoints Mac Connector 1.8.2

Bugfixes/Enhancements

- Fixed a bug introduced in 1.8.0 that could cause the AMP service to restart unexpectedly.
- Fixed a kernel panic on macOS 10.12 when accepting TCP connections from malicious hosts. (CSCvk08192)
- Disabled unsupported command line capture when running on OS X 10.11 and earlier.
- Improved command line capture with macOS 10.12.4 and later.
- Improved Support Tool command line arguments, descriptions, and optimized data collected when generating a support snapshot.
- Improved file execute activity monitoring to ensure appropriate SHA value generation.
- Corrected display of policy information when Connector starts without network connection.
- Updated third party libraries including changes related to these vulnerabilities (CSCvij56731):
  - ClamAV:
    - CVE-2017-12380
    - CVE-2017-12379
    - CVE-2017-12378
    - CVE-2017-12377
    - CVE-2017-12376
    - CVE-2017-12375
    - CVE-2017-12374
    - CVE-2017-11423
    - CVE-2018-0361
    - CVE-2018-0360
  - Curl:
    - CVE-2018-1000300
    - CVE-2018-1000301
    - CVE-2018-1000122
    - CVE-2018-1000121
    - CVE-2018-1000120
  - SQLite:
13 June 2018 Release Notes

• CVE-2018-8740

**IMPORTANT!** We strongly advise Mac Connector 1.3.0 users to upgrade to 1.3.1 then reboot the system before upgrading to 1.8.2. Upgrading directly from 1.3.0 to 1.8.2 may cause a kernel panic.

**IMPORTANT!** If your Connectors are deployed with Mac Connector v1.8.0, we recommend upgrading to v1.8.2. If you previously disabled the command line capture feature due to the v1.8.0 announcement regarding Connector restarts, you can reenable the command line capture feature after completing the upgrade.

13 June 2018 Release Notes

Private Cloud Administration Portal 2.4.4

**New**

• Added the ability to surface data around bad cloud lookups within support snapshots.

**Bugfixes/Enhancements**

• Fixed an issue where certain cloud lookups with bad data sent by integrations were not stored in the database, so no retrospectives could be performed on these lookups.

• Increased the performance of the Events page by limiting the size and frequency of certain large events.

25 April 2018 Release Notes

AMP for Endpoints Windows Connector 5.1.15

**New**

• Added /kb4072699 installer switch to automatically set the registry key necessary to receive the Windows Security Update for KB 4072699.

**IMPORTANT!** Test and ensure compatibility of all AV products installed before using this installer switch. See Cisco AMP for Endpoints Compatibility with Windows Security Update KB4056892 for important details in the Caveats and Considerations section that apply to use of the installer switch for setting the registry key.
Bugfixes/Enhancements

- Improved compatibility with TrendMicro (CSCvi07080).
- Addressed a Clam AV issue that was triggering false positive detections against PDF files (CSCvi01400).
- Fixed an issue where Windows Connector updates may fail with password protection enabled.
- Patched a DLL hijacking vulnerability in the Connector installer (CVE-2017-12312).
- Extremely long process command line arguments are now properly captured.
- The Connector UI accurately displays Cloud connectivity status.
- Improved ability of the Connector to detect and repair configuration issues during regular usage and on Connector upgrade.
- Improved performance of Process Exclusions for operating systems prior to Windows Vista.
- Addressed an issue where the Connector is unable to upgrade directly from version 5.0.9 or older to 5.1.11 when Connector Protection is enabled.
- Reliability of Support Package generation has been improved.
- Connector will not generate new identity on machines where the BIOS serial number contains white spaces.
- Addressed issue where the Connector service does not automatically start after multiple upgrades without a reboot.
- Improved security of the Connector Protection password.
- Improved Windows proxy discovery.
- Improvements to make Connector upgrades more robust going forward.
- Addressed an issue where the Connector would leave many temporary files behind, filling up the disk.
- The History page on the Connector user interface now shows the proper detection name for quarantined files that were already in the local cache.
- Improved reliability when an Endpoint IOC scan is launched.
- Updated SQLite version to prevent high CPU usage.
- Improved Connector user interface responsiveness.
- Connector service now functions properly when installed on Windows 10 Fall Creators Update.
- The Connector no longer causes a warning to appear when opening the Computer Management window.
- Improved TETRA file detection parsing. (CSCvh54783, CSCvh77705)
- Addressed an issue where the Connector could cause a blue screen under rare conditions. (CSCvh56811)
- Fixes for multiple Clam AV vulnerabilities:
  - CVE-2017-6420
  - CVE-2017-12378
  - CVE-2018-0202
25 April 2018 Release Notes

• CVE-2017-6418

IMPORTANT! Starting from Windows Connector 5.1.13, we will no longer be supporting the addition of new features for Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008 (non-R2) operating systems. Critical bug fixes and security patches will still be made to the 5.x.x branch of the Connector for a limited time. For more information, please refer to the End of Support Announcement.

AMP for Endpoints Mac Connector 1.7.0

New
• Digitally signed malware will now be quarantined by the Mac Connector.
• Support macOS High Sierra (10.13).
• Resume filesystem scans after AMP service daemon restarts.
• Hide exclusion list in UI based on policy configuration.
• Added automatic crash reporting.
• ClamAV virus definition file versions are now displayed.

IMPORTANT! The AMP for Endpoints Mac Connector no longer supports OS X 10.10 and earlier as of version 1.7.0.

Bugfixes/Enhancements
• Improved DMG container handling.
• Addressed race condition that would result in failed quarantine restores.
• Custom or scheduled scans that result in 0 files being scanned no longer report as a failed scan.
• Installs of the Connector on a system with multiple users will no longer be incorrectly reported as failed.
• Remove old quarantined files automatically.
• Restrict access permission of some internal files.
• Update Third Party libraries.
• Fix memory leak.
• Optimize how exclusions are applied.
• Improve Cloud Recall Restore error handling.
• Scan full contents of archives that contain malware.
• Addressed memory leak when scanning plist files.
• Fixed potential crash during a failed retrospective quarantine.
• Fixed a bug that caused retrospective quarantine failure events to be displayed even though it succeeded.
• Improved compatibility with macOS 10.13.
• Updated third-party libraries.
25 April 2018 Release Notes

- Reclassified some error messages that were being logged frequently under normal circumstances so they are only seen when running the Connector with Debug Logging enabled in policy.
- Increased the size of the retrospective database from 50MB to 500MB with better pruning efficiency to decrease disk reads and writes.
- Reduced disk write activity. (CSCvd15950)
- Reduced the number of duplicate network detection events sent.
- Enhanced scanning of larger files on execution.
- Improved formatting of information in the UI.
- Added SupportTool option for specifying maximum size of output archive.
- Reclassified error messages that can be logged frequently under normal operation.
- Updated third party libraries.
- Patched ClamAV vulnerabilities:
  - CVE-2018-1000085
  - CVE-2012-6706
  - CVE-2017-6419
  - CVE-2017-6418
  - CVE-2017-6420
  - CVE-2018-0202

AMP for Endpoints Linux Connector 1.7.0

New
- Update Linux signed file quarantine guardrail.
- Resume filesystem scans if the daemon restarts.
- Hide exclusion list in UI based on policy configuration.
- Remove old quarantined files automatically.
- Official support for RHEL/CentOS 7.4.
- Official support for RHEL/CentOS 6.9.
- ClamAV virus definition file versions are now displayed.

Bugfixes/Enhancements
- ClamAV vulnerability fixed.
- Update 3rd party libraries.
- Bypass proxy when unable to connect to AMP registration server.
- Fix execute not being excluded from scan when it should be.
- Fix custom scan misbehavior.
- Disable unintended auto-start of ampmon after reboot in CentOS 6.
- Scan full contents of archives that contain malware.
- Do not treat directed or scheduled scans which processed zero files as failed.
- Fix restore from quarantine failure.
• Fix CLI crash when displaying very long exclusion lists.
• Fix intermittent failure where CLI is stuck in initializing phase.
• Fixed HTTP parsing for certain processes.
• Improved upgrade process to protect against failures.
• Fixed a bug that caused retrospective quarantine failure events to be displayed even though it succeeded.
• Updated third-party libraries.
• Reclassified some error messages that were being logged frequently under normal circumstances so they are only seen when running the Connector with Debug Logging enabled in policy.
• Increased the size of the retrospective database from 50MB to 500MB with better pruning efficiency to decrease disk reads and writes.
• Fixed installation failure when the system temporary directory is mounted without execute permission.
• Fixed issue where the system may hang during start up due to kernel module conflict.
• Reduced disk write activity.
• Reduced the number of duplicate network detection events sent.
• Enhanced scanning of larger files on execution.
• Removed CLI history file from user home directory on full uninstall.
• Added SupportTool option for specifying maximum size of output archive.
• Improved the handling of network mounted drives by the SupportTool.
• Improved CLI display formatting.
• Reclassified error messages that can be logged frequently under normal operation.
• Updated third party libraries.
• Patched ClamAV vulnerabilities:
  • CVE-2018-1000085
  • CVE-2012-6706
  • CVE-2017-6419
  • CVE-2017-6418
  • CVE-2017-6420
  • CVE-2018-0202
15 November 2017 Release Notes

Private Cloud Administration Portal 2.4.2

Bugfixes/Enhancements

• Fixed a bug where retrospective data was not processed in some situations.

FireAMP Console 5.3.20171105

Bugfixes/Enhancements

• Fixed a bug where some data displayed in an integrated Firepower Management Center may not reflect current endpoint network addresses.
• Fixed a bug where running ipsupporttool.exe on a computer after installing AMP for Endpoints Windows Connector 5.1.11 will temporarily disable File Fetch functionality on the endpoint.

24 October 2017 Release Notes

Private Cloud Administration Portal 2.4.1

Bugfixes/Enhancements

• Fixed an issue where Disposition Server - Extended Protocol registration fails if proxy authentication is set to none.
• Fixed an issue where slow DNS causes a timeout when registering with the Disposition Server - Extended Protocol.
• Relaxed certificate validity requirements.
• Fixed an issue that could cause increased memory use and impact stability.
• Fixed issues where files were not submitted for Threatgrid analysis from integrated FMC, ESA, and WSA devices.
• Fixed an issue where vulnerable applications were not being alerted on.
• Fixed issues related to malicious file detection on integrated FMC, ESA, and WSA devices.

AMP for Endpoints Windows Connector 5.1.11

**IMPORTANT!** Upgrading to 5.1.11 from a 4.4.5 or earlier Connector will fail if Connector Protection is enabled. To upgrade you must disable Connector Protection in Policies and wait for the policy to be applied to your Connectors before upgrading. Connector Protection may be re-enabled once the upgrade has succeeded. This will be fixed in the next Connector release.
Private Cloud Administration Portal 2.4.0 (superseded by 2.4.1)

New

- Added the Disposition Server - Extended Protocol to support advanced Connector features.

**IMPORTANT!** A migration wizard has been added to transition to the Extended Protocol. To deploy new Connectors you must first migrate to the Extended Protocol. Only upgrades from previous versions of Private Cloud need to run the migration wizard.

- Improved interface for certificate management.

Bugfixes/Enhancements

- Fixed a bug where a Private Cloud device in Air Gap mode could not enable remote file fetch due to Two Step Verification issues. Contact support to enable this.
- Advanced Custom Detections are now downloaded over HTTPS.
- Resolved an issue where backup size increased dramatically under some use cases.
- Addressed various security issues.

FireAMP Console 5.3.20170823

New

- AMP for Endpoints Linux Connector is now available for download in your Private Cloud device.

Bugfixes/Enhancements

- Fixed an issue with Identity Sync.
- Low Prevalence Executables will now display correctly when used in conjunction with rules-based access control.
AMP for Endpoints Windows Connector 5.1.11

New

- Disposition Server - Extended Protocol has been enabled in the Connector.
- Limited rebranding from Sourcefire FireAMP to Cisco AMP for Endpoints.

**IMPORTANT!** As part of the rebranding, the Connector default installation path was changed to C:\Program Files\Cisco\AMP. Before upgrading your endpoints to this version, be sure to review any exclusions you have for 3rd party software that is installed alongside AMP for Endpoints.

- Updated the TETRA engine to add support for downloading signature deltas.
- A new Timed Diagnostic Tool option is available in the Cisco AMP for Endpoints Connector Start Menu group.
- A utility to test connectivity from the endpoint to the Private Cloud device is now included in the installation directory.
- Connector binaries are now signed using the Cisco EV code signing certificate.
- The AMP for Endpoints Windows Connector can now be installed on systems that have Secure Boot enabled.

**IMPORTANT!** Starting from Windows Connector 6.0.1, we will no longer be supporting the addition of new features for Windows XP, Windows Vista and Windows Server 2003 operating systems. Critical bug fixes and security patches will still be made to the 5.x.x branch of the Connector for a limited time. For more information, please refer to the End of Support Announcement.

Bugfixes/Enhancements

- Updated TETRA license key.

**IMPORTANT!** The TETRA license for all Windows Connector versions prior to 5.1.11 will expire on November 1, 2017. If you wish to continue using the TETRA engine you must upgrade before this date.

- The DFC driver now initializes more reliably.
- The Connector now has an increased window for monitoring network connections.
- The local DFC cache is now being updated correctly.
- Certain IP ranges are no longer incorrectly whitelisted by the Connector.
- Custom IP black/whitelist entries composed of CIDR block and port number combinations are now processed correctly by the Connector.
- The Connector Protection password is no longer logged during the uninstall process.
- Unnecessary TETRA definitions are no longer downloaded when the local definition set is up to date.
- Reduced the likelihood of the Connector generating a new identity on upgrade.
- Scanning of container files (pdf, zip, tar, etc) is now more robust.
- Improved accuracy of parent process reporting.
- Performance of process exclusions has been improved.
- Patched a vulnerability in unrar (CVE-2012-6706)
- Addressed an issue where Connectors installed on Windows SMB servers would cause shared, mapped drives to be inaccessible.
- Addressed issues where the Connector could lose connection to the Private Cloud device when Identity Sync is enabled.
- Addressed an issue where the Connector could be disabled by a user with admin privileges when Connector Protection is enabled.
- Addressed a crash that would occur when attempting to enable debug logging.
- Fixed a crash that could occur during the Connector service shutdown.
- Addressed an issue where a password containing certain special characters was not being parsed correctly when attempting to uninstall the Connector via command line with Connector Protection enabled.
- Improved system performance when the Connector is installed on systems with VMware Persona Management.
- Addressed an issue where the Connector could cause a BSOD under rare conditions.
- Fixed an issue where the Connector could cause system freezes in some instances.
- Addressed an issue with Endpoint IOC scans consuming high amounts of CPU.
- The Connector is now able to download TETRA definitions over SSL.
- Added a fix to address a vulnerability in bzip2 (CVE-2016-3189).
- Removed erroneous log lines that appeared when using the Connectivity Test Tool.
- Improved stability of the Connector by addressing numerous reported crashes.
- Improved handling of local configuration files to reduce instability due to configuration errors.
- Addressed issue where the Connector network driver could cause a BSOD when Windows Driver Verifier is used against it.
- Modified altitude of the AMP for Endpoints Windows drivers to be more in line with Microsoft software recommendations.
- Addressed an issue where the Connector could become deadlocked.
- Addressed compatibility issues with LabLogic Debra.
- Addressed an issue where virtualized systems were not correctly being identified as unique.
- Addressed an issue where the installer would not complete successfully under certain circumstances.
- Addressed an issue where previously downloaded TETRA definitions couldn’t be used after a partial uninstall followed by a re-install.
- Addressed an issue where the Connector would not shut down in a timely fashion while TETRA definitions were being downloaded.
- Fixed an issue where Application Blocking events were not reporting parent process information properly.
• Addressed an issue where log files could grow beyond their maximum size.
• Fixed an issue where the Connector would continue to apply Advanced Custom Detection definitions after they were removed from policy until the Connector was restarted.
• Fixed an issue where HDB Advanced Custom Detection signatures would not be correctly applied when configured to use a wildcard for file size.
• Addressed an issue where the first scan after install would execute without network activity or before TETRA definitions were fully downloaded.
• Addressed an issue where the Connector would negatively impact write performance when installed on machines with solid state drives (SSDs).
• Addressed an issue on Windows XP where the Connector could not acquire the machine's IP address when configured with a static IP address and the “Register this connection's addresses in DNS” option was disabled.
• Updated curl to version 7.51.0.
• Addressed a vulnerability where Connector Protection could be bypassed during uninstall by entering a specific character in the password field.
• Improved the ability for the Connector to upgrade/uninstall connectors that are in a crashed state.
• Fixed an issue where TETRA could incorrectly flag files as malicious.
• Fixed an issue where TETRA was not handling the detection of malicious archive files properly in certain situations.
• Fixed a rare issue where the Connector would cause high CPU usage due to MTU and policy size.
• Addressed an issue where the Connector process was able to be stopped via debugger access.
• Users are now able to configure which path to store temporary files during the installation process through a command line switch.
• Improved the uninstall process to better handle scenarios where the Connector is in a bad state prior to uninstalling.
• Improved overall stability of the Connector.
• Addressed a minor issue where the Connector would report a successful custom scan for invalid paths.
• Improved error reporting.

**IMPORTANT!** Upgrading from certain Connector versions will require a reboot. Downloading the new installer or performing an update via policy will provide a list of computers in the selected group or policy that will require a reboot.
AMP for Endpoints Mac Connector 1.4.3

New

- Disposition Server - Extended Protocol has been enabled in the Connector.
- Added Support for Mac OS X 10.12.

**IMPORTANT!** Users running macOS 10.12 (Sierra) should upgrade to 10.12.4 or later. There are compatibility issues that affect system stability which are resolved in macOS 10.12.4.

- Rebranded product from Sourcefire FireAMP to Cisco AMP for Endpoints.
  As part of the rebranding, the Connector installation paths have changed to:
  - /Applications/Cisco AMP
  - /Library/Application Support/Cisco/AMP for Endpoints Connector
  - /opt/cisco/amp
  Before upgrading your endpoints to this version, be sure to review any exclusions you have for 3rd party software that is installed alongside AMP for Endpoints.
- Added support for Advanced Custom Detections.
- A command line interface has been added to the AMP for Endpoints Mac Connector. This can be used to initiate scans, sync policies, show the Connector history, and more.
- The Connector will now send queries for LZMA compressed Adobe Flash files, MSO attachments within MS Office 2003 XML files, and Hancom Office files.
- Added scanning of files referenced by startup and launch related plists.
- Upgraded ClamAV engine to 0.99.2.

**IMPORTANT!** The AMP for Endpoints Mac Connector no longer supports OS X 10.7 as of version 1.3.0.

Bugfixes/Enhancements

- Addressed issue where a different folder may be inadvertently deleted during the uninstall process when a subdirectory in the “/Users” directory contains a subdirectory with a space character.
  Note that most systems are not affected as macOS System Preferences prevents creating a user with a space character in the account name.
  To trigger this issue, two similarly-named user directories must exist (e.g. “/Users/JohnDoe” and “/Users/JohnDoe Copy”). If “/Users/JohnDoe Copy” contains the path to AMP Connector log files (e.g. “/Users/JohnDoe Copy/Library/Logs/Sourcefire”), uninstalling or upgrading will result in the user directory “/Users/JohnDoe” being deleted.
- Fixed a bug in the AMP network kernel extension that can cause a kernel panic.
- Patched a vulnerability in unrar (CVE-2012-6706)
30 August 2017 Release Notes

- Applied security fixes from 3rd party libraries used by the Connector including OpenSSL, cURL, and xmlsec.
- Fixed a bug where a user-initiated scan could interfere with detections in real-time file operations.
- Strengthened guards against misbehaving UI clients.
- Fixed a bug to ensure that files found to be malicious by the offline engine are scanned using the Private Cloud device before generating a detection event.
- Fixed a bug where file paths are included in queries even when the feature is disabled in policy.
- Fixed a bug causing a “too many open files” error after parsing MSXML files.
- Fixed a bug where user information for some events are missing.
- Fixed a bug causing a UI lockup when performing flash scan.
- Improved the readability of quarantine failure messages.
- Improved resiliency against corrupt ClamAV definition files.
- Removed a dependency on perl in the installer.
- Resolved an issue where the connector could not quarantine malicious resource forks.
- Applied security fixes from third party libraries including OpenSSL, Jansson and Libxml2.
- Fixed a bug that stopped ClamAV from scanning files when disconnected from the Private Cloud device.
- Addressed an issue where certain file activity could cause scans to stop prematurely.
- Fixed a bug where files contained inside PDF files were not scanned.
- Fixed a bug where some UDP connections were not monitored.
- Fixed a bug where user information was missing from some events.
- Fixed a bug where some deferred scans were dropped because the deferred scan file was not written to correctly.
- Fixed a bug where the URL reported for some network events were malformed.
- Fixed a bug where Definition Update events were missing from the Events table.
- Fixed a bug where the known viruses count for Definition Update events was incorrect.
- Made automatic ClamAV definition updates more robust.
- Clarify in Execution Blocked events and notifications that no action was taken when the Connector is running in audit mode.
- Removed stale files from ClamAV working directory at daemon start-up.
- Reduced the performance overhead of wildcard exclusions.
- Fixed a bug where a kernel extension could panic if there are active network connections when the daemon is stopping or retrying a failed initialization step.
- Fixed various logging issues.
- Updated curl version to 7.51.0.
- Addressed an issue where the Connector would consume high CPU when a local database reached a certain size.
- Fixed a bug where the Connector would consume high CPU when some local 3rd party software would periodically touch but not modify files.
• The Connector is now able to successfully quarantine files that have immutable flags set.
• Addressed various issues with scan error reporting.
• Fixed an issue where you could not fetch a file from a computer after it was deleted even if other copies of the same file existed on the computer.
• Addressed an issue where the Connector would only perform a Retrospective Quarantine on the first instance of a file on the computer.
• Fixed a bug where scans in progress when the computer was rebooted did not appear to complete in the Console.
• Fixed an issue where outdated ClamAV definitions were still being loaded by the Connector in some instances. This could potentially cause an increase in false-positive detections.
• Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
• Modified the Connector installer to prevent downgrades when running the installer locally.
• Added more diagnostic information collected by the Support Tool.
• Improved performance when using Application Blocking lists on Mac OS X 10.8 and 10.9.
• Improved handling of nested archive files.
• Fixed an issue where the Connector was not sending information about the current user for certain events.
• Fixed an issue where the Connector wasn’t cleaning up its child processes.
• Improved overall Connector stability and efficiency.
• Addressed issue where ClamAV would download definitions more often then necessary.
• Resolved issue where Connector sent extraneous file execute events.
• Addressed various memory usage issues.
• Improved DFC engine to robustly handle network events.
• Improved file move event detection data for better representation in Device Trajectory.
• Fixed issue where the connector was not clearing the file scan queue in some cases.
• Improved various UI messages and error notifications.
• Improved messaging for events displayed in the management console.
• Improved error messaging when attempting a custom scan for an invalid path.
• Improved Connector upgrade functionality and console notifications.
• Connector updated to dynamically honor file scan size limits on policy change.
• Fixed various issues with exclusion handling.
• Improved handling of archive files.
• Improved ability of the connector to handle malicious forking executable files.
• Improved Connector compatibility for OS X 10.10 and above.
• Addressed issue where upgrading OS X with the Connector installed would sometimes freeze the system.
30 August 2017 Release Notes

- Improved Connector performance when installing from read-only media (e.g. DVDs).
- Addressed issue where cache TTLs were not expiring as expected.
- Changed Support Package creation process improving efficiency and flexibility.
- Added ability to specify custom output path for Support Package using “-o” option.

AMP for Endpoints Linux Connector 1.3.1

New
- Disposition Server - Extended Protocol has been enabled in the Connector.
- Added support for Red Hat Enterprise Linux and CentOS 7.2 and 7.3
- Added support for Red Hat Enterprise Linux and CentOS 6.7 and 6.8.
- Added support for Advanced Custom Detections.
- ClamAV upgraded to 0.99.2.
- The Connector will now send queries for LZMA compressed Adobe Flash files, MSO attachments within MS Office 2003 XML files, and Hancom Office files.

Special Advisory
Important note for RHEL and CentOS 6.0–6.5 users
Confirm the installed version of procps is 3.2.8-30 or newer prior to installing this update. Older versions of procps are not compatible and users are advised to update to the latest version. Refer to the following Red Hat advisories for details:

https://rhn.redhat.com/errata/RHBA-2016-0904.html
3 August 2017 Release Notes

Private Cloud Administration Portal 2.3.6

New

• An alert (see below) has been added to the Administration Portal about the upcoming Private Cloud 2.4 release.

FireAMP Console 5.3.20170728

New

• An alert (see below) has been added to the FireAMP Console about the upcoming Private Cloud 2.4 release.

Upcoming Private Cloud v2.4 Release Alert

AMP Private Cloud v2.4 includes a new AMP Cloud protocol allowing us to bring more features to the AMP platform. Upgraded installs must run the included migration wizard to use the new AMP Cloud protocol.

IMPORTANT! To continue using the TETRA engine you must migrate to the new AMP Cloud protocol and upgrade to AMP for Endpoints Windows Connector version 5.1.11.

The following TechZone article describes the full set of changes and benefits of migrating to the new AMP Cloud protocol.

http://cs.co/amppc24release
14 June 2017 Release Notes

Private Cloud Administration Portal 2.3.5

Bugfixes/Enhancements
• Fixed an issue where certain event types could cause the Events page to freeze.

11 May 2017 Release Notes

Private Cloud Administration Portal 2.3.4 (superseded by 2.3.5)

Bugfixes/Enhancements
• Resolved a performance issue by tuning an internal data store.
• Fixed a problem when automatically applying content updates.

IMPORTANT! A migration process has been added that must be completed after upgrading from previous versions to 2.3.3. The migration can take 12 to 24 hours and during this time Connectors will be unable to perform lookups against the device.
8 March 2017 Release Notes

Private Cloud Administration Portal 2.3.2

Bugfixes/Enhancements
- Fixed an issue relating to retrospective and cloudlogs cron jobs. This only affects devices that have been updated, not fresh installs.

FireAMP Console 5.3.20170202

Bugfixes/Enhancements
- Fixed an issue where email from Event Subscription notifications were not being sent.

14 February 2017 Release Notes

Private Cloud Administration Portal 2.3.1

Bugfixes/Enhancements
- Fixed an issue where content updates fail when a proxy server is configured.
- Fixed an issue with excessive TokuMX logging.
- Fixed an issue where a logrotate cron job could interfere with backups.
- Limited the number of mysql binlog files to 15 to guard against filling up the /data partition.

FireAMP Console 5.3.20170202

Bugfixes/Enhancements
- Fixed an issue where immediate email from event notifications were not being sent.
- Updated documentation to include AMP for Endpoints Mac Connector for OS X 10.11 and 10.12.
- Fixed an issue where reports could timeout and create empty PDFs.
8 December 2016 Release Notes

Private Cloud Administration Portal 2.3.0

New
• New field in the Integrations tab for VirusTotal.
• UI Change for the Administration Portal to include Cisco Web Security Appliance integration.

Bugfixes/Enhancements
• Default collection has been removed from Storage Configuration.
• Defence Center has been renamed to Firepower Management Center.
• Validation added to Threat Grid hostname.
• AMP Threat Grid integration now has show/hide buttons for the TG API key input field.
• Disposition update service password is now user configurable.
• Cloud server is renamed to Disposition server.
• Customizable From, Sender Name, and Device Name fields for notification emails.
• Bugfix to content updates which handles new yum behavior.
• Better help messages displayed for Firepower Management Center (formerly DC) Integration page.
• Support snapshots now contain additional information.
• The Server Keys upload form has been hidden when on a default (non-custom) upstream Disposition Server.
• SSL Keys page in the Administration Portal now shows data for default generated certs and user uploaded certificates.

FireAMP Console 5.3.20161013

New
• Added an API Credentials page to simplify 3rd party application management.
• The FireAMP API allows you to make changes to your business. API users can move computers, assign policies to groups, and make modifications to Application Blocking and Simple Custom Detection lists.
• New Reports are available under the Analysis heading. Old reports are still available.
• VirusTotal integration is enabled in proxy mode to allow files to be compared to VirusTotal on the right-click context menu. This must be enabled in the Administration Portal.
• Users can now specify their timezone so dates and times will be displayed in the chosen timezone throughout the Console.
• Clicking a date entry anywhere will show a pop-up menu with additional options.
• Added global search to the menu bar throughout the Console. This is the same as available under the Analysis header.
• Added filters to the Audit Log page. Added User links that will take you to a filtered view of the Audit Log.
• You can now select which VM operating system image to use for Cisco AMP Threat Grid file analysis.
• Added information about reboot requirements to Product Update section of Policies and to the Download Connector page.

Bugfixes/Enhancements
• File Analysis page now displays threat report score on each result line.
• Fixed a bug that caused policy updates to fail in certain situations.
• Added Event Type filters for product updates.
• Fixed a bug that caused the incorrect file type to be displayed in trajectory data.
• Redesigned the Audit Log page for usability.
• Moved version number to Help dialog.
• Added support for Hangul Word Processor files. These files will now appear in File and Device Trajectory and can be submitted for File Analysis.
• The SHA-256 of archive files are now displayed when a detection is triggered by a file contained within the archive.
• Clarified detection events when a Connector is in a group with a policy that uses Audit Mode.
• Fixed a bug where Advanced Custom Detections (ACD) were unable to add zmd signature.
• We now report the last policy serial number that a Connector reported in with in the Device Trajectory.
• Fixed a bug where some events weren’t showing in the dashboard unless filtered by GUID/computer.
• There is a new error code for consecutive agent crashes.
• Fixed a bug where cached File Trajectory data was being served to all users regardless of rules based access and control.
• Fixed a bug where aggregate IP Lists could fail silently.

AMP for Endpoints Windows Connector 4.4.5

New
• Starting with upgrades from version 4.4.3 to future versions, the AMP for Endpoints Windows Connector no longer requires a reboot after every update.

IMPORTANT! Updates that include major functionality changes or bugfixes may still require a reboot.

• Added support for Windows 10.
8 December 2016 Release Notes

- The endpoint IOC scanner now supports the ability to only catalog changes in the filesystem, allowing IOC scans to complete faster after the first full catalog has been completed.
- AMP for Endpoints Windows no longer requires Windows administrator credentials for scheduled scans.

Bugfixes/Enhancements
- TETRA definitions can now be downloaded when the Connector is configured to use a proxy server.
- Addressed a bug where TETRA definition downloads did not appear to complete successfully even though they did.
- Fixed a rare issue where the Connector would cause high CPU usage due to MTU and policy size.
- Addressed security issue where the Connector process was able to be stopped via debugger access.
- Addressed security issue where Connector Protection could be bypassed on uninstall.
- Addressed issues where the Connector install would occasionally fail.
- Enhanced scope of Endpoint IOC flash scan indexing to provide increased coverage. Please refer to the Cisco Endpoint IOC Attributes document for more information.
- Improved performance during the Endpoint IOC collection phase to reduce collection time.
- Addressed an issue where IOC Flash Scans were not correctly cleaning up files from previous scans.
- You can now stop the Connector service via the command line when Connector Protection is enabled.
- Made improvements to the installer for preserving previous command line options.
- Various stability improvements and bugfixes.
- Improved Connector reliability during installation and upgrades.
- The Connector now dynamically honors file scan size limits when changed in policy. Previously the Connector service would have to be stopped and restarted.
- Improved handling of archive files.
- Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types.
- Fixed an issue where the Connector was not sending information about the current user for certain events.
- Fixed a problem where the Connector was not reporting the parent file type correctly in some cases.
- Fixed a bug where .elf file was not being found by windows agent but is being convicted by Mac.
AMP for Endpoints Mac Connector 1.0.10

**IMPORTANT!** Mac connectors need to use port 32137 instead of 443, this is configurable via policy.

Bugfixes/Enhancements
- Fixed an issue where the Connector could register with the FireAMP Console without an IP address.
- Addressed issue where the Connector could potential get deadlocked and not be able to recover.
- Added new CPIO Archive (OLD), Master Boot Record, and GUID Partition Table File types.

6 September 2016 Release Notes

Private Cloud Administration Portal v2.2.3

Bugfixes/Enhancements
- Adjusted internal memory configuration for improved performance.
- Fixed a potential deadlock in the disposition service.
- Addressed an issue that could result in event data not being correctly stored.
- Performance enhancements to FireAMP Console when dealing with large amounts of historical data.

AMP for Endpoints Windows Connector v4.1.9

Bugfixes/Enhancements
- Addressed an issue where policy updates could fail with specific endpoint MTU values.

9 August 2016 Release Notes

Private Cloud Administration Portal v2.2.2

Bugfixes/Enhancements
- Fixed an issue in Air Gap mode where a content update would fail when applied.
- Addressed an issue in Air Gap mode where updates could fill the data partition on the Private Cloud device.
31 May 2016 Release Notes

• Addressed a bug in Air Gap mode where content updates were not queuing input files for retrospective.
• Fixed a Proxy Mode issue where content updates were not automatically being downloaded and applied when Apply/Install was selected from the Updates page.

31 May 2016 Release Notes

Private Cloud Administration Portal v2.2.1

Bugfixes/Enhancements
• Corrected an erroneous link in online help.

AMP for Endpoints Windows Connector v4.1.7

Bugfixes/Enhancements
• Patched ClamAV engine to address vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
• Addressed an issue where the TETRA engine was generating false-positive detections.

AMP for Endpoints Mac Connector v1.0.9

Bugfixes/Enhancements
• Patched ClamAV engine to address vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
• Addressed a rare issue where the Connector logs could grow continually without bounds.

17 May 2016 Release Notes

Private Cloud Administration Portal v2.2.0

New
• FireAMP Private Cloud now supports integration with Cisco AMP Threat Grid appliances.
• FireAMP Private Cloud now supports integration with Cisco ESA version 10.0 and higher.
Bugfixes/Enhancements

- Added FIPS-compliant TLS keys for the disposition server.
- Fixed a /tmp directory unmount error during reboot.
- Added a glibc fix for CVE-2015-7547.
- Fixed a problem with restores failing because the root directory was filled during restore from backup.
- Fixed an issue where the Private Cloud device loses boot configuration after a power failure.
FireAMP Console v5.2.20160509

New
• File Analysis is now available when a Cisco AMP Threat Grid Appliance is integrated with your Private Cloud device. This allows analysis of files in the File Repository and automatic analysis of Low Prevalence Executables.

Bugfixes/Enhancements
• Policies automatically update after a license renewal, which adds updated certificates.

AMP for Endpoints Windows Connector v4.1.6

Bugfixes/Enhancements
• Updated protocol version to support new TLS keys.

3 February 2016 Release Notes

Private Cloud Administration Portal v2.0.4

New
• Added notification about upgrading to Private Cloud version 2.1.

18 December 2015 Release Notes

Private Cloud Administration Portal v2.1.0

New
• Replaced MongoDB with TokuMX, this results in performance and reliability gains.

IMPORTANT! To upgrade to version 2.1 existing customers must backup their version 2.0 Private Cloud device and restore it during the version 2.1 install.

• New and improved performance metrics.
• New notification on upstream cloud server ping failure.
• New hardware requirements page with shutdown VM option.
• Under new live support session, support identity is a click to expand.
18 December 2015 Release Notes

Bugfixes / Enhancements

• Release notes for code updates are displayed in the Administration Portal.
• Default options for “Support Snapshot” when in airgap mode.
• Updated warning dialog on password change.
• Removed the errors tab from any areas that stream logs. Instead the errors are merged with the output.
• Change log added to software update details.
• Backups now use a .bak extension.
• Improved the option to replace a Private Cloud device license.
• Changed the scheduled backups pop-up when storage configuration is too large.
• Network settings page has been rearranged.
• Installation steps have been rearranged.

FireAMP Console v5.2.20151203

New

• Endpoint Indication of Compromise (IOC) feature added. You can filter based on the Endpoint IOC state and also activate, deactivate, and delete Endpoint IOCs in bulk.
• Added the ability to create administrator and unprivileged user accounts in the FireAMP Console. Administrators can assign unprivileged users access to view groups, edit policies, and create and edit outbreak control lists.
• Added an option to subscribe to individual event alert emails.
• Vulnerable Software functionality added. If an executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database that information is displayed on the Vulnerable Software page.
• Added the ability to search for computers by Connector GUID.
• Export computer details to a CSV file from the Computers page.
• Added the ability to request file from any deployed FireAMP Connectors.

IMPORTANT! You must have Two-Step Verification enabled on your account to request files from your Connectors and download them from the File Repository. Files can only be fetched from computers running version 4.1.2 or later of the AMP for Endpoints Windows Connector and version 1.0.6 of the AMP for Endpoints Mac Connector.

Bugfixes / Enhancements

• Added the ability to bulk delete computers from the Computers page.
• Improved bulk move operations on the Computers page.
• The Computers page can now be filtered by the last time an endpoint connected to the Cloud.
18 December 2015 Release Notes

• Added a new UI feature to view all dates and timestamps in various formats by right-clicking the date to open a context menu.
• Fixed cross-site scripting issues on several pages.
• Added Group Filter to Dashboard, Threat Root Cause, and Deployment Summary pages that allow the view to be filtered based on selected Groups.
• Redesigned and consolidated the FireAMP Connector download page.
• Added Maximum Scan File Size and Maximum Archive Scan File Size items to AMP for Endpoints Windows Connector policies.
• SHA-256 values on File Repository page are now color-coded based on disposition.
• Removed Verbose Notifications policy item from AMP for Endpoints Mac Connector policies.
• Improved Groups page interface, including creating and editing groups.
• All user actions on Advanced Custom Detection lists are now recorded in the Audit Log.
• AMP for Endpoints Mac Connector policies updated to improve cloud query efficiency.
• Upgraded AMP for Endpoints Mac Connector protocol version to improve compatibility and reliability.
• Performance improvements to Device Trajectory load times.
• Fixes on various list pages and reports for when users who created the lists or reports have been deleted. The creator of these lists will now show as unknown.
• Fixed auto refresh on the Dashboard Overview tab.
• Redesigned Computers page with new computer view. You can now filter the view and move multiple computers to new Groups.
• Redesigned Users page with new layout. You can now search user accounts by name and email address and quickly access your own account.
• Better identification of Computers page for running scans for individual computers.
• Removed On Copy Mode and On Move Mode policy items and made these settings Passive for all FireAMP Connectors.
• Removed Unseen Cache TTL policy item as this was not used by the FireAMP Connector.
• Fixed an issue where event filters containing special characters could cause a javascript exception.
• Users can now specify a different email address to receive notifications.
• First Use wizard can now be accessed after initial setup from the Management > Quick Start menu item.
• Enhancements to Search page for better quality and clarity of results.
• Redesigned Business page.
8 October 2015 Release Notes

AMP for Endpoints Mac Connector v1.0.7

Bugfixes / Enhancements
- Added support for OS X 10.11
- Addressed issues causing Time Machine backups to take a long time over AFP.
- Fixed an issue where the Connector would block applications while in Audit mode.
- Optimized Flash Scans for faster performance.
- Various bug fixes.

8 October 2015 Release Notes

AMP for Endpoints Windows Connector v4.1.5

New Features
- Addressed an issue where the Connector could become disconnected from the cloud. The computer may appear as a newly installed Connector in the default group if this problem occurs. AMP for Endpoints Windows Connector version 4.1.2.10076 is affected.

8 September 2015 Release Notes

Private Cloud Administration Portal v2.0.20150904

New Features
- Added ISO split and reassembly functionality to the amp-sync utility.

Bugfixes / Enhancements
- Added guardrails to the amp-storage-container command to prevent accidental deletion of the /data container.
- Various bugfixes.

AMP for Endpoints Windows Connector 4.1.2

New Features
- ClamAV engine updated to version 0.98.5.
- TETRA engine updated to version 3.0.0.71.
8 September 2015 Release Notes

Bugfixes / Enhancements

- Improved efficiency of the exclusion engine when handling wildcard exclusion types.
- Fixed a bug that would cause the Connector crash reporting tool to fail.
- Fixed an issue where the Connector would crash if left in debug mode for an extended period of time.
- Added enforcement of size limits for Connector log files to a maximum of 10 files, each up to 50MB in size at any given time.
- Advanced Custom Detections can now be dynamically applied without restarting the Connector.
- Improved error reporting during policy update failures.
- Connector uninstall events are now properly reported from behind a proxy.
- Connector is now able to perform Identity Synchronization from behind a proxy.
- Fixed a bug where the Connector could crash when scanning certain file types.
- Fixed a vulnerability where an unprivileged user could cause the Connector to crash through the UI.
- Fixed a bug where using the Microsoft Application Verifier tool could cause the Connector to crash.

AMP for Endpoints Mac Connector 1.0.6.292

New Features

- Added the ability to specify the output path of Support Packages with a command line parameter.
- AMP for Endpoints Mac Connector officially certified on OS X 10.10.
- Added Event History, Policy View, Local Scanning, and Headless Mode to the user interface.

IMPORTANT! If the user interface is not visible on a Connector after the update, check the Start Client User Interface setting in your policy.

Bugfixes / Enhancements

- Performance improvements in the file scanning engine for more efficient calculation of file hashes and ClamAV scanning.
- Eliminated incorrect notifications when attempting a manual policy sync through the endpoint UI.
- Resolved issue where erroneous log messages appeared at system startup.
- Less ambiguous endpoint notifications by displaying “Off-line” when system is not connected to a network or the interface is disabled and “Service Unavailable” if there are problems connecting to the cloud.
- Addressed compatibility issue with OS X mail.app where malicious emails are continually downloaded and quarantined by the AMP for Endpoints Mac Connector. The Connector now detects and notifies that malicious emails are present but does not quarantine malicious .emlx files created by mail.app. It is
left to the administrator to remove the malicious email from the server manually. If mail.app is configured to automatically download attachments and those are determined to be malicious, the Connector will continue to quarantine those attachments.

**IMPORTANT!** This fix only affects OS X mail.app. Other email applications may behave differently.

- Resolved a rare issue where the Connector is unable to sync policies for some period of time.
- Addressed a performance issue where users experienced high CPU usage after waking the computer from sleep or performing a reboot.
- Fixed high CPU usage issues on OS X 10.10 due to changes in Spotlight.
- Eliminated a race condition where kernel extensions were unable to successfully unload on shutdown or reboot.
- Improved Connector validation of user-created exclusions.
- Fix for a WebDAV kernel panic issue.
- Fix for a race condition that would cause policy update failures.
- Significant performance improvement from file event queue optimization.
- Compatibility update for OS X 10.10 related to the metadata indexer.
- Cleanup of erroneous Connector syslog messages.
- Added notifications for Device Flow Correlation, definition updates, Cloud Recall, and product updates.
- Updated ClamAV library to support scanning raw DMG files.
- Performance improvements.
- Various fixes for support cases.

---

**Private Cloud Administration Portal v2.0.20150525**

**Bugfixes / Enhancements**

- Included a patch for the June 30, 2015 leap second.
- Improved user interface for device and content updates.
- Enhanced proxy support for retrieving updates.
Private Cloud Administration Portal v2.0.20150325205338

New Features
  • FireAMP Private Cloud now supports air gap deployments.

Bugfixes / Enhancements
  • Fixed an issue where disk performance and usage graphs were shown for removable devices.
  • Fixed an issue where gaps in data were causing incorrect values for query failure rates.
  • Added a sanity check for devices with insufficient memory.
  • Additional information is now collected for support snapshots.
  • Memory allocations for services are automatically adjusted based on VM memory at boot time.
  • Patch for June 30, 2015 leap second.
24 February 2015 Release Notes

Private Cloud Administration Portal v1.5.20150206133846

Bugfixes / Enhancements
  • Upgraded AMP for Endpoints Mac Connector protocol version to improve compatibility and reliability. This update is required to ensure future connectivity between the Private Cloud device and AMP for Endpoints Mac Connectors. All AMP for Endpoints Mac Connector policies will be updated to enable this change.

29 January 2015 Release Notes

AMP for Endpoints Windows Connector 3.1.17.9685

Bugfixes / Enhancements
  • Fixed an issue where saving an Excel file to a network drive could take an unusually long time.

Private Cloud Administration Portal v1.5.20150126112807

Bugfixes / Enhancements
  • Improve accuracy for Private Cloud Administration Portal metrics reporting.

8 January 2015 Release Notes

FireAMP Console v4.5.2014112012

Bugfixes / Enhancements
  • Resolved an issue with restoring quarantined files from the FireAMP Dashboard.

FireAMP Cloud Server 0.9.17-1

Bugfixes / Enhancements
  • Resolved an issue with storage of cloud server lookups.

7 November 2014 Release Notes
8 October 2014 Release Notes

FireAMP Console v4.5.2014110616

Bugfixes / Enhancements
• Performance improvements for file disposition lookups in Device Trajectory.

AMP for Endpoints Windows Connector 3.1.16

Bugfixes / Improvements
• Fixed a bug caused by the accumulation of archived ClamAV logs that could result in computers running out of disk space. Archived ClamAV logs are now deleted hourly.

8 October 2014 Release Notes

Private Cloud Administration Portal v1.5.20141002

Bugfixes / Enhancements

18 September 2014 Release Notes

Private Cloud Administration Portal v1.5.20140916

Bugfixes / Enhancements
• Support for Cloud Recall functionality when a Defense Center is connected to Private Cloud.

AMP for Endpoints Windows Connector 3.1.11

Bugfixes / Enhancements
• Fixed translation error in the Japanese version of the AMP for Endpoints Windows Connector.

20 August 2014 Release Notes

Private Cloud Administration Portal v1.5.20140814
Bugfixes / Enhancements
• Fixed a problem that would sometimes cause content updates to fail.
• Fixed a bug that would cause report generation to fail.
• Increased minimum RAM requirement for the Private Cloud VM to 16GB when the OVA is first installed.

Private Cloud Administration Portal v1.5

New Features
• Added integration with Cisco Defense Center.

Bugfixes / Enhancements
• Fixed bug associated with growing storage containers from the same disk.
• Refresh DNS when switching from DHCP to static.
• Disabled multiple support sessions.
• Validate proxy server information.
• Fixed bug where an HTTP 502 response was returned after 40 seconds.
• Updated OpenSSL to address recent vulnerabilities including Heartbleed.

FireAMP Console 4.5.20140306

New
• Two-Step Verification will be an available option for all users.
• AMP for Endpoints Mac Connector now available.

Bugfixes / Enhancements
• Detailed file information can now be accessed from the File Trajectory page either by search or by right-clicking the filename or SHA-256 value.
• A single default exclusion set is now created during first use rather than one each for Audit, Protect, and Triage policies.
• Address an issue where policy scheduled scans created in the month of January would fail to run.
• New favicon for the FireAMP console.
• Added new Indication of Compromise event called Generic IOC to flag suspicious behavior.

AMP for Endpoints Windows Connector 3.1.11
• Updated TETRA license key to avoid expiry on July 1, 2014.