AMP for Endpoints Release Notes

2017

5 December 2017

AMP for Endpoints Windows Connector 6.0.5

New

- Exploit Prevention detection engine to block exploits and memory attacks that target certain processes.
- System Process Protection adds protection for memory attacks against certain Windows system processes.
- This version of the Connector runs on Windows 7, Windows 8 and 8.1, Windows 10, Windows Server 2008 R2, and Windows Server 2012. Older versions of Windows are no longer supported.

IMPORTANT! On Windows 7 and Windows Server 2008 R2 you must apply the patch for Microsoft Security Advisory 3033929 before installing the Connector.

Bugfixes Since the Exploit Prevention Beta Connector Release:

- 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.

5 December 2017

Bugfixes/Enhancements:

- Fixes for multiple ClamAV vulnerabilities.
- 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.

IMPORTANT! All upgrades from previous AMP for Endpoints Windows Connector versions to 6.x.x will require a reboot of the endpoint.

AMP for Endpoints Console 5.4.20171205

New

- Added Process Exclusion type to support System Process Protection in AMP for Endpoints Windows Connector version 6.0.5 and later.
- Added Policy settings to enable Exploit Prevention and System Process Protection in AMP for Endpoints Windows Connector version 6.0.5 and later.

IMPORTANT! All policies must be on the new AMP Cloud infrastructure by running the Cloud Migration tool before you can deploy AMP for Endpoints Windows Connector version 6.0.5 and later. All new policies created since February 2016 use the new AMP Cloud infrastructure by default.

Bugfixes/Enhancements

- Added Connector version numbers to the Download Connector page. After you select a Group the Connector version to be downloaded will be displayed for each Connector type.

30 November 2017

AMP for Endpoints Mac Connector 1.5.1

Bugfixes/Enhancements

- Fixes for multiple ClamAV vulnerabilities.
- Addressed memory leak when scanning plist files.
- Fixed potential crash during a failed retrospective quarantine.

AMP for Endpoints Linux Connector 1.5.1

New

- Official support for RHEL/CentOS 7.4.
- Official support for RHEL/CentOS 6.9.

Bugfixes/Enhancements

- Fixes for multiple ClamAV vulnerabilities.
- Fixed HTTP parsing for certain processes.

28 November 2017

AMP for Endpoints Console 5.4.20171128

New

- You can send users a notification to set up Two-Step Verification.
- New filters added to Users page: Last Login, Two-Step Verification, Remote File Fetch, and Command Line.
- A CAPTCHA is displayed when a user has many failed login attempts.
- New UI for improved Policy configuration.
- Command line data is now available on the API.
- Businesses in the EU can now switch their AMP for Endpoints accounts to use the new EU Threat Grid Cloud.
- Individual users can now be configured with permission to view command line data.

- New popover on clicking IP addresses, URLs, and SHA-256s.
- Enable scanning of Word, PowerPoint, and Excel file types in AMP for Endpoints Mac and AMP for Endpoints Linux Connector policies.

31 October 2017

AMP for Endpoints Console 5.4.20171031

New

- Updated menu colors to be more consistent with other Advanced Threat products.
- Users can now specify Windows 10 as the OS to run analysis on when sending files to the Threat Grid.
- Users can now chose to preview the new Policy UI. The existing policy UI will be deprecated soon.
- Password requirements are now more stringent.
- New Splunk app is now in the Splunk app store.
  https://splunkbase.splunk.com/app/3670/#/details
  https://splunkbase.splunk.com/app/3686/#/details

18 October 2017

AMP for Endpoints Linux Connector 1.5.0.518

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.

Bugfixes/Enhancements

- 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.

17 October 2017

AMP for Endpoints Mac Connector 1.5.0.548

New

- Support macOS High Sierra (10.13).
- Resume filesystem scans after AMP service daemon restarts.
- Hide exclusion list in UI based on policy configuration.

Bugfixes/Enhancements

- 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.
- Remove old quarantined files automatically.
- Restrict access permission of some internal files.

5 October 2017

AMP for Endpoints Windows Connector 5.1.13

IMPORTANT! Starting from Windows Connector 6.0.1, 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.

Bugfixes/Enhancements

- 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 blank spaces.
- Addressed issue where the Connector service does not automatically start after multiple upgrades without a reboot.
- Improved reliability of system reboot after upgrades in Windows Server 2003.

28 September 2017

AMP for Endpoints Console 5.4.20170928

New

- Reorganized top bar navigation:
  - Support link is now in the Help menu.
  - My Account and Log Out links are now located in the new User menu.
- Auto-Refresh on Dashboard - To better help customers viewing the Dashboard on large screens (for example in a Network Operations Centre), the Dashboard page can now be set to auto-refresh.

24 August 2017

AMP for Endpoints Mac Connector 1.4.5

New

- Digitally signed malware will now be quarantined by the Mac Connector.

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.

9 August 2017

AMP for Endpoints Console 5.4.2017080915

New

- User Name Search feature.
- Allow user to select the AMP Threat Grid VM to use when sending a file for analysis.

Bugfixes/Enhancements

- Fixed a bug in the Product Updates section on the Edit/Create Policy page where Connector version numbers were not sorted correctly.
- Fixed a bug where search results that were shas displayed the incorrect context menu.
- Addressed an issue where inbox events were not grouped correctly.

3 August 2017

AMP for Endpoints Mac Connector 1.4.3

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.

IMPORTANT! Mac Connector 1.4.2 will no longer be made available in the portal.

If you installed 1.4.2, you must upgrade to 1.4.3 directly without uninstalling 1.4.2.

If you downloaded the 1.4.2 installer, it is recommended that you replace it with a 1.4.3 installer immediately.

AMP for Endpoints Windows Connector 5.1.11

IMPORTANT! Starting from Windows Connector 6.0.1, 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.

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 to supplement the cloud-based protection of the Windows Connector, 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 allow listed by the Connector.
- Custom IP block/allow list 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.

18 July 2017

AMP for Endpoints Linux Connector 1.3.1

Bugfixes/Enhancements

- Patched a vulnerability in unrar (CVE-2012-6706)
- Patched a vulnerability in curl (CVE-2017-7468)

11 July 2017

AMP for Endpoints Console 5.4.20170711

New

- The Cisco AMP for Endpoints terms (previously the EULA) have been updated for consistency across the entire Cisco portfolio. The latest version of the Cloud terms can be found at http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html

Bugfixes/Enhancements

- Changed the Groups list on the Connector download page to be sorted alphabetically.
- (API only) The Executed Malware indication of compromise event includes extra fields like filename and path where available.
- Fixed a bug where policy serial numbers could be incremented incorrectly under certain circumstances.
- Deleted computers are no longer included in the computer count on the Automatic Analysis page.
- Addressed an issue where there could be a discrepancy between the number of licensed computers and the number of computers shown on the Computers page.

6 July 2017

AMP for Endpoints Windows Connector 5.1.9

Bugfixes/Enhancements

- Patched a vulnerability in unrar (CVE-2012-6706)

AMP for Endpoints Mac Connector 1.4.2 (superseded by 1.4.3)

IMPORTANT! AMP for Endpoints Mac Connector 1.3.0 users are strongly advised to upgrade to 1.3.1 then reboot the system before upgrading to 1.4.2. Upgrading directly from 1.3.0 to 1.42 can cause a kernel panic. For more information, please refer to this special advisory.

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.

6 July 2017

New

- Rebranded product from Sourcefire FireAMP to 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 localization support to the Connector UI for Simplified Chinese, Japanese, and Korean.

Bugfixes/Enhancements

- Fixed a bug in the AMP network kernel extension that can cause a kernel panic.
- Patched a vulnerability in unrar (CVE-2012-6706)
- Fixed a bug where connection to the AMP cloud may fail when SSL inspection is enabled on the network gateway.
- 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 AMP cloud before generating a detection event.
- Fixed a bug where file paths are included in cloud 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 the AMP daemon may crash after disconnecting from the AMP cloud for an extended amount of time.
- 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.

20 June 2017

AMP for Endpoints Console 5.4.20170620

New

- Added custom filters and alerting to the Dashboard and Inbox tabs so users can receive email alerts for new compromises.
- Added WannaCry demo data and associated document.

Bugfixes/Enhancements

- Added Windows 7 Japanese and Korean operating systems as options for File Analysis. Windows XP and Windows 7 32-bit operating systems are no longer supported by File Analysis. If you currently have your default image set to one of these on your Business page the default will automatically change to Windows 7 x64.

8 June 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.7

Bugfixes/Enhancements

- Addressed an issue where Connectors installed on Windows SMB servers would cause shared, mapped drives to be inaccessible.

6 June 2017 Release Notes

AMP for Endpoints Console 5.4.20170606

New

- Added support for single sign-on through Active Directory, Okta, and Ping Federate.
- Added a policy option to hide list of exclusions from the AMP for Endpoints Windows Connector UI on versions 5.1.3 and higher.

Bugfixes/Enhancements

- Prevalence now shows data based on a global list of prevalence instead of only your deployment.
- The default values of some policy items have changed when creating new policies:
  - Heartbeat Interval is set to 15 minutes.
  - Send User Name in Events is enabled.
  - Hide File Notifications is enabled.
  - Maximum Scan File Size is set to 50 MB.
  - Maximum Archive Scan File Size is set to 50 MB.
- Command Line Logging policy item is only available when Connector Log Level is set to Debug and Command Line Capture is enabled.
- Default Windows exclusions have been updated when creating a new exclusion set.

1 June 2017 Release Notes

AMP for Endpoints Mac Connector 1.3.1

Bugfixes/Enhancements

- This special release fixes a defect in AMP for Endpoints Mac Connector version 1.3.0 that can cause an unexpected system restart. It is highly recommended that 1.3.0 users upgrade to this version and restart their systems before attempting to upgrade to newer Connector versions. Users currently running 1.2.6 or earlier are encouraged to skip this version and upgrade to newer versions directly.

  Refer to advisory AMP for Endpoints Mac Connector 1.3.0 Defect Can Cause Unexpected System Restart for details.

9 May 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.5

Bugfixes/Enhancements

- Addressed issues where the Connector could lose connection to the cloud 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.
- Addressed a minor issue when multiple quarantine notifications are shown on the endpoint for Korean operating systems.

2 May 2017 Release Notes

AMP for Endpoints Console 5.4.20170502

New

- Added computer description drop-down to Device Trajectory.
- Added Send User Name in Events to Policies for Mac Connector (version 1.3.0 and later)
- Added Send User Name in Events to Policies for Linux Connector (version 1.1.1 and later)

4 April 2017 Release Notes

AMP for Endpoints Console 5.4.20170404

New

- Added process exclusions for AMP for Endpoints Windows Connector 5.1.3 and higher.

Bugfixes/Enhancements

- Added pagination for Significant Compromise Artifacts on Dashboard and Inbox tabs.
- Added the ability to mute Significant Compromise Artifacts on Dashboard and Inbox tabs.
- Added the ability to view details of Significant Compromise Artifacts on Dashboard and Inbox tabs.
- Added file names for SHA-256 artifacts on Dashboard and Inbox tabs.
- Added install_date timestamp to the Computers API so users can see the install dates of Connectors.

4 April 2017 Release Notes

AMP for Endpoints Linux Connector 1.3.0

New Features

- Added support for Red Hat Enterprise Linux and CentOS 7.2 and 7.3

Bugfixes/Enhancements

- Fixed a bug where connection to the AMP cloud may fail when SSL inspection is enabled on the network gateway.
- 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 AMP cloud before generating a detection event.
- Fixed a bug where file paths are included in cloud queries even when the feature is disabled in policy.
- Fixed a bug causing " too many open files" error after parsing MSXML files.
- Fixed a bug where the AMP daemon may crash after disconnecting from the AMP cloud for an extended amount of time.
- Fixed a bug where user information for DFC detection events are missing.
- Improved the readability of quarantine failure messages.
- Improved resiliency against corrupt ClamAV definition files.
- Added abrt crash reports to the Support Tool diagnostic archive.

3 April 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.3

New Features

- The Connector will now register with Windows Security Center when TETRA is enabled via policy and all definitions have completed downloading.

Bugfixes/Enhancements

- 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.
- Fixed an issue where altitudes of older Connectors that are upgraded to 5.1.1 or higher were not modified to be more in line with Microsoft software recommendations.
- The Connector is now able to download TETRA definitions over SSL.
- Fixed an issue on Windows XP where the migration from 'Sourcefire' to 'Cisco' install directories was not working correctly when upgrading from versions prior to 5.1.1.
- Addressed an issue where Cloud Notifications were displayed by default when installing the Connector without an injected policy.
- Added a fix to address a vulnerability in bzip2 (CVE-2016-3189).
- Removed erroneous log lines that appeared when using the Connectivity Test Tool.

7 March 2017 Release Notes

AMP for Endpoints Console 5.4.20170307

Bugfixes/Enhancements

- Added Compromise Event Types to the Dashboard and Inbox tabs.
- Fixed a bug in Applications integration to better align Computer IPs between the AMP for Endpoints Console and Firepower Management Console.
- Authentication server changes will redirect users to a new host when logging in. Any pending password resets may have to be resent.

16 February 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.1

New

- Limited rebranding from Sourcefire FireAMP to 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.

- Added localization support to the Connector UI for Simplified Chinese, Japanese, and Korean.
- Updated the TETRA engine to add support for downloading signature deltas.
- A new Timed Diagnostic Tool option is available in the AMP for Endpoints Connector Start Menu group.
- A utility to test connectivity from the endpoint to the Cisco cloud 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.

Bugfixes/Enhancements

- 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 VMWare View Persona Management and 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.

Release note links

Current release notes can be found here.

Other release notes can be found at the following links:

- 2020 release notes
- 2019 release notes
- 2018 release notes
- 2016 release notes
- 2015 release notes
- 2014 release notes
- 2013 release notes