AMP for Endpoints Release Notes

2019

17 December 2019

AMP for Endpoints Windows Connector 7.1.5

Bugfixes/Enhancements

- Fixed an Exploit Prevention engine issue that could cause Google Chrome v78 and later to crash or display a renderer code integrity error.
- Made stability improvements in the Connector installer.

16 December 2019

AMP for Endpoints Linux Connector 1.12.0 (superseded by 1.12.7)

New

- Improved Connector authentication when connecting to AMP Cloud services.

Bugfixes/Enhancements

- Fix restart issue when scanning CIFS mounts with Kerberos authentication. (CSCvs45576)
- Updated ClamAV to 0.102.1, including changes related to the following vulnerability:
  - CVE-2019-15961

AMP for Endpoints Mac Connector 1.12.0 (Superseded by 1.12.7)

New

- Improved Connector authentication when connecting to AMP Cloud services.

Bugfixes/Enhancements

- The " Connector requires reboot" fault is no longer raised on macOS 10.13 and 10.14.
- Updated fault remedy screens for macOS 10.15 Catalina full disk access and system extension faults.
- Reduced install time when using Active Directory/LDAP.
- Updated ClamAV to 0.102.1, including changes related to the following vulnerability:
  - CVE-2019-15961

10 December 2019

AMP for Endpoints Console 5.4.20191210

New

- Effective January 2020, Console Audit logs will contain 3 years of historical data.

5 December 2019

AMP for Endpoints Windows Connector 7.1.1

New

- Added support for the Windows 10 November 2019 Update (version 1909).
- Upgrading and uninstalling the Windows Connector no longer require a reboot under most conditions.

> **IMPORTANT!** No reboot upgrades only apply when upgrading from Connector version 7.x.x to a later version. While most upgrades will not require a reboot, there may be occasional instances where a reboot is still required.

Bugfixes/Enhancements

- Stability improvements in the Exploit Prevention engine.
- Endpoint Isolation improvements that fix sync issues between the Console and Connector.
- Stability improvement for the Protect driver.
- Addressed an Endpoint IOC engine crash for non-English versions of Windows (CSCvs09940).
- Updated curl to v7.66.0.
- Updated ClamAV to 0.101.4. This version addresses the following vulnerabilities:
  - CVE-2019-1010305
  - CVE-2019-12625
  - CVE-2019-12900
- Resolved Exploit Prevention engine compatibility issues with the following applications:
  - SAP SSO Addon
  - Microsoft Excel 2016
  - XLSLINK software
- During an Endpoint Isolation session if you enter the unlock code incorrectly 5 times you will not be able to make another attempt to unlock it again for 30 minutes.

26 November 2019

AMP for Endpoints Console 5.4.20191126

Bugfixes/Enhancements

- Demo Data computers now show the latest Connector version and supported Operating System. You must refresh Demo Data to see these changes.
- The Last Seen time for Demo Data computers now matches the time it was enabled or refreshed.
- Endpoint Isolation is now available on Demo Data computers. The group policy for the Demo Data computers must have Endpoint Isolation enabled. Endpoint Isolation is available for Windows Connector versions 7.0.5 and later.
- Redesigned Single Sign-On configuration page.

12 November 2019

AMP for Endpoints Console 5.4.20191112

New

- AV Definitions Threshold in the Business Settings page lets you configure a grace period for computers' AV definitions before they appear as out of date on the Computer Management page.
- There is a new option for the Last Seen filter: "Within 7 Days".
- You can use the Audit Logs API to retrieve audit logs.
- Added a new field called av_update_definition in the rest API response for single computer queries that include AV version and status values.

Bugfixes/Enhancements

- Fixed a bug that prevented forensic snapshot files from downloading properly.

29 October 2019

AMP for Endpoints Console 5.4.20191029

Bugfixes/Enhancements

- You can use wildcards when performing searches on the Computers page.

28 October 2019

AMP for Endpoints Linux Connector 1.11.1

New

- Added official support for RHEL/CentOS 7.7.
- Added kernel modules built with a Retpoline-enabled compiler for RHEL/CentOS 6.

Bugfixes/Enhancements

- Fixed a rare crash on RHEL/CentOS 7 which could occur when monitored files on a network drive were removed. (CSCvr43285)
- Updated ClamAV to 0.101.4, including changes to address the following vulnerabilities:
  - CVE-2019-1010305
  - CVE-2019-12625
  - CVE-2019-12900

15 October 2019

AMP for Endpoints Console 5.4.20191015

New

- All links in the console for additional information about Common Vulnerabilities and Exposures (CVE) direct to the National Vulnerability Database at https://nvd.nist.gov instead of Cisco Security.
- Endpoint Isolation – A spinner in the UI indicates status changes in progress.
- The Business pages under the Accounts menu have been combined into a single Business Settings page.
- You can directly access License Information from the Accounts menu.

Bugfixes/Enhancements

- Beta – Only administrators have access to Orbital policy. Unprivileged users cannot enable or disable Orbital.

10 October 2019

AMP for Endpoints Mac Connector 1.11.1

New

- Added official support for macOS 10.15 Catalina. This release supports macOS 10.13, 10.14, and 10.15.

Bugfixes/Enhancements

- Updated ClamAV to 0.101.4, including changes related to the following vulnerabilities:
  - CVE-2019-1010305
  - CVE-2019-12625
  - CVE-2019-12900

8 October 2019

AMP for Endpoints Windows Connector 7.0.5

New

- Endpoint Isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation.
- System Process Protection notifications
  - are less verbose. (CSCvn41948)
  - are no longer sent when the process in question is excluded by process exclusions. (CSCvo90440)

BugFixes/Enhancements:

- A failing System Process Protection rule no longer prevents the Self Protect driver from starting.
- Endpoint indication of compromise (IOC) driver stops gracefully when uninstalling Windows Connector.
- Upgraded curl version to fix an integer overflow vulnerability in NTLM password authentication (CVE-2018-14618).
- Memory leak fixes and other stability improvements in the Self-Protect driver.
- Malicious Activity Protection engine no longer incorrectly detects Google Chrome.
- Windows Connector gathers the BIOS serial number more reliably when it is needed to detect hardware changes for registration with AMP Cloud.
- Windows Connector Crash is now handled by the Cisco Security Connector Monitoring Service (CSCMS) Server.
- Fixed an issue where currently running rootkit scans continued to run after the Connector service was stopped.
- Fixed incompatibility with Kaspersky Real-Time Engine.
- Improved stability of the Exploit Prevention engine.
- New certificate for the Early Launch Antimalware (ELAM) driver.
- Reduced false positives with the Malicious Activity Protection engine.
- Fixed issue where the support tool would sometimes fail to include all necessary files.
- Fixed a crash on shutdown issue.
- Windows Connector support package is now a ZIP file instead of 7zip so that Windows can natively unpack the support package.

1 October 2019

AMP for Endpoints Console 5.4.20191001

New

- Beta - Endpoint Isolation IP Allow lists: there is a new Endpoint Isolation IP Allow list type under **Outbreak Control** > **Network - IP Block & Allow Lists**.
  - IP lists with no ports and less than 200 IP addresses that are connected to Endpoint Isolation in policies will be migrated; IP lists that don't meet these criteria will not be migrated and will need to be recreated as Endpoint Isolation IP Allow lists and added to the Endpoint Isolation policy.
  - Policies and groups using the Endpoint Isolation IP Allow lists will appear in the IP List details panel. All new IP allow lists for Endpoint Isolation must be created using this new list type.

Enhancements

- Unprivileged users can now use Casebook and access the pivot menu next to their observables in the AMP console.
- Users now have the ability to delete a group using the REST API.
- Windows Connector engine notifications can now be easily hidden from the user on the endpoint. All engine notifications on the Windows Connector policy pages are condensed into one check box called **Engine Notifications**. The default for this feature is off. Note that If you previously hid one of the engine notifications, all engine notifications are now set to hidden.

18 September 2019

AMP for Endpoints Windows Connector 6.3.7

Bugfixes/Enhancements

- Fixed Exploit Prevention engine access violation issue which crashed the Connector.
- Resolved Exploit Prevention engine compatibility issues with the following applications:
  - Kronos ERP add-on (CSCvq76698)
  - ExOpen plug-in (CSCvq73086)
  - .NET applications (CSCvq74953)
  - Adobe Acrobat (CSCvq46250)

17 September 2019

AMP for Endpoints Console 5.4.20190917

New

- Beta – Details for computers show the recent isolation history and make it easier to find unlock codes when manually stopping isolation.
- Beta – A new version of the Connector (7.0.3) is available for download from the Endpoint Isolation section of the Beta page. The upgrade from 7.0.1 to 7.0.3 does not require a reboot to complete.

IMPORTANT! To continue testing the Endpoint Isolation beta feature, you must install Connector 7.0.1 or 7.0.3 from the Beta Features page. See the Endpoint Isolation beta guide for full beta features and change details.

3 September 2019

AMP for Endpoints Console 5.4.20190903

New

- Beta – New Endpoint Isolation policy setting: Allow DNS. See the Endpoint Isolation beta guide for details.
- Beta – New Endpoint Isolation policy setting: Allow DHCP. See the Endpoint Isolation beta guide for details.
- Beta – New Endpoint Isolation policy setting: Allow use with proxy. See the Endpoint Isolation beta guide for details.
- Beta – There is a link to the Endpoint Isolation overview video in the Inbox and the Beta Features page.

Bugfixes/Enhancements

- Beta – Endpoint Isolation state stays synchronized between the Connectors and the console.
- Diagnostics button in Device Trajectory now works reliably.
- Fixed a bug where computers could be moved out of the beta group through the API.

IMPORTANT! To continue testing the Endpoint Isolation beta feature, you must uninstall existing 6.5.1 Connectors and install the new beta Connector (7.0.1) from the Beta Features page. See the Endpoint Isolation beta guide for details.

20 August 2019

AMP for Endpoints Console 5.4.20190820

Bugfixes/Enhancements

- Beta – Simplified the Endpoint Isolation details that are displayed in Events page, Computers page, and Device Trajectory.

6 August 2019

AMP for Endpoints Console 5.4.20190806

New

- Beta – Users are notified that any ports specified in IP lists for Endpoint Isolation will have no effect. (All ports will be allowed.)

Bugfixes/Enhancements

- Beta – Audit log entries for Endpoint Isolation are more consistent with other audit log entries.

23 July 2019

AMP for Endpoints Console 5.4.20190723

New

- Password changes are now processed through the Cisco Security Account page. Password complexity requirements have been updated as a result.
- Beta – Calls to start, stop, and retrieve Endpoint Isolation status are available in the API.
- Beta – Endpoint Isolation activity is now displayed in the audit log.
- Beta – Non-administrator users can be given permission to start, stop, and update Endpoint Isolation.

22 July 2019

AMP for Endpoints Linux Connector 1.11.0

New

- Added support for Process Exclusions. See AMP for Endpoints: Process Exclusions in macOS and Linux for more information.
- Added lightweight Linux-only ClamAV definition configuration option. See AMP for Endpoints: ClamAV Virus Definition Options in Linux for more information.

Bugfixes/Enhancements

- Changed virus definition update download protocol from HTTP to HTTPS.
- Improved performance when processing execute-triggered scans.
- Improved performance on systems with multiple mount namespaces.
- Fixed incorrect known virus count in virus definition update event.
- Fixed install failure due to error creating new user group.
- Fixed memory leak affecting systems with low filesystem and network activity.
- Fixed memory leak that may occur after a detection event.
- Fixed memory leak that may occur after applying virus definition update.

AMP for Endpoints Mac Connector 1.11.0

New

- Added support for Process Exclusions. See AMP for Endpoints: Process Exclusions in macOS and Linux for more information.

Bugfixes/Enhancements

- Improved detection events to include download source URL when available (CSCve69181).
- Changed virus definition update download protocol from HTTP to HTTPS.
- Fixed incorrect known virus count in virus definition update event.
- Fixed memory leak affecting systems with low filesystem and network activity.
- Fixed memory leak that may occur after a detection event.
- Fixed memory leak that may occur after applying virus definition update.
- Improved UI stability.
- Updated third party libraries.

18 July 2019

AMP for Endpoints Android Connector 1.1.0

New

- Built with more recent Android tools and SDK.
- Conforms to Android background execution limitations on Android 8.0 and later.
- Updated UI uses Cisco branding.

Bugfixes/Enhancements

- Uninstall functionality now works on Android 9.0 and later.
- Initial Scan no longer fails on phones with Secure Containers (for example, Samsung Secure Folder).
- Initial scan for notification event and on-screen event are now in sync.
- Fixed native library error on Android 7.0 and later.
- Minor UI changes/fixes.

10 July 2019

AMP for Endpoints Windows Connector 6.3.5

BugFixes/Enhancements

- Fixed Cisco AMP for Endpoints crash on startup when Windows Management Instrumentation (WMI) service is disabled. (CSCvq39434)
- Improved Exploit Prevention engine with added protection against BlueKeep security vulnerability discovered in Microsoft's Remote Desktop Protocol. (CVE-2019-0708)
- Resolved Exploit Prevention engine compatibility issue with the following applications:
  - WIDOS Application
  - Micro Focus Unified Functional Testing (UFT) Application (CSCvq18773)
  - Insider Threat/Web Insider (CSCvq09279)

9 July 2019

AMP for Endpoints Console 5.4.20190709

Bugfixes/Enhancements

- Device Trajectory icons now show properly in the Chrome browser.

- Command line capture text has been changed from green to gray to avoid confusion with process status text.
- IP list items with a CIDR block of /32 are displayed without the CIDR notation on the IP list edit pages.
- Fix to prevent attempting to create a snapshot on unsupported connectors.

27 June 2019

AMP for Endpoints Windows Connector 6.3.3

Bugfixes/Enhancements

- Fixed Cisco AMP for Endpoints Windows Command Injection Vulnerability (CVE2019-1932, CSCvp53361).
- Resolved compatibility issue with Kaspersky Real-Time Engine which prevented it from starting (CSCvq22483).
- Resolved Exploit Prevention engine compatibility issues with these applications:
  - Internet Explorer with VBScript running on local machine (CSCvo91932)
  - Adobe add-on PitStop Pro
  - Intel HD Graphics
  - Outlook add-on iManage
  - Excel plugin KuTools v19 - 64bit/32bit (CSCvq02201)
  - Nuance EditScript MT 11 (CSCvq02237)
  - Symantec PGP (CSCvq02223)
  - Symantec DLP Plugin (CSCvq02211)
  - SKYSEA Client (CSCvp84312)
  - AppV container

25 June 2019

AMP for Endpoints Console 5.4.20190625

New

- Two-step verification has been renamed to two-factor authentication.
- The button to notify a user to enable two-factor authentication is now located under Settings on the user account page.
- Beta - Endpoint Isolation start/stop events now display the user who triggers the event.
- Beta - Endpoint Isolation APIs have been added.
- Beta - Endpoint Isolation Status has been added as a filter to Computers page.
- Beta - Endpoint Isolation IP list size is now limited to 200 entries.

Bugfixes/Enhancement

- Vulnerabilities API endpoint queries now return results filtered by an inclusive start date and an exclusive end date.
- Calling the REST API with invalid JSON will now return a 400 error code.

11 June 2019

AMP for Endpoints Console 5.4.20190611

New

- Vulnerabilities API now enables you to filter by group GUID.
- Vulnerabilities API now enables you to get a list of computers with a specific vulnerable application by passing the SHA-256 of the application.
- The SHA-256 field for Mac and Linux Process exclusions has been removed to improve performance.
- Beta - Endpoint isolation details are now displayed in Device Trajectory.
- Beta - Trajectory API now displays endpoint isolation events.

Bugfixes/Enhancements

- Vulnerabilities API calls now honor AMP RBAC.
- Deleting exclusions from an exclusion set now appears in the audit log.

28 May 2019

AMP for Endpoints Console 5.4.20190528

New

- Users can now create an IP list by uploading a CSV file containing IP addresses/CIDR blocks.
- Added a REST API for querying vulnerabilities observed in the last 30 days.

Bugfixes/Enhancements

- Fixed issue where some buttons were inaccessible when using Internet Explorer.
- Improved validation messages for errors when entering multiple IP addresses.

14 May 2019

AMP for Endpoints Console 5.4.20190514

New

- Users can now edit and manage their IP lists in the console.
- Added support in Windows policies for new file types for cloud lookup (changes will take effect on next update to policy):
  - 7ZSFX
  - XML_WORD
  - XML_XL
  - XML_HWP (Hangul)
  - HWP3 (Hangul)
  - OOXML_HWP (Hangul)
  - HWPOLE2 (Hangul)
  - MBR

7 May 2019

AMP for Endpoints Windows Connector 6.3.1

New

- Added support for Windows 10 May 2019 Update (Version 1903) (Preview build: 18362.53).
- New Cisco Anti-Malware Protected Process Light (AM-PPL) services “Cisco Security Connector Monitoring Service(CSCMS)” to register with WSC on Windows 10 19H1 and beyond.
- New installer command line switch to skip registration and startup of Connector in order to use the Windows operating image as a deployable golden image:
  - `/goldenimage = 1` (Skip initial Connector registration and startup on install)
  - `/goldenimage = 0` (Do not skip initial Connector registration and startup on install)
- Now supports scanning Windows shortcut (.lnk) and RAR5 compressed file types.

Bugfixes/Enhancements

- Fixed BSOD caused when Connector, under some circumstances, incorrectly requests a file to be quarantined from a different volume than where it was originally detected. (CSCvo11650)
- Fixed incompatibility with MS Sysprep.
- Connector now supports launching the AMP UI from WSC, and also shows statuses. (CSCvo61707)
- Windows Connector Installer can now handle special characters in the install path. (CSCvk54455)
- Windows Connector no longer protects itself when the Connector service is set to ‘disable’, thereby allowing users to modify the Connector’s service status. (CSCvj72318)
- Fixed logic around deleting quarantine files that exceed the TTL and have already been deleted. (CSCvo00165)
- Added a new check for the end-of-file on non-Microsoft file systems which will prevent a custom app from hanging when running through a network share with Windows Connector installed.
- Stopped Malicious Activity Protection (MAP) from monitoring network drives (CSCvo32112)
- Addressed an issue where the Connector could cause a BSOD in MAP driver under rare conditions (CSCvp03825)
- Fixed Exploit Prevention engine from blocking Windows 10 updates
- Resolved Exploit Prevention engine compatibility issue with below applications
  - MS Excel plugin Aspen
  - Fasoo DRM

    - Trusteer Rapport
    - ivanti application
    - MS Excel plugin ResQ
    - Tavos Taxport web app
    - MalwareBytes AV
    - Java installer.
- Update ClamAV to 0.101.2, including addressing below security vulnerabilities
    - CVE-2019-1787
    - CVE-2019-1788
    - CVE-2019-1789
- Enhanced IDSync logic to prevent Windows Connector from falling back to the default group (CSCvo23266)

30 April 2019

AMP for Endpoints Mac Connector 1.10.2

Bugfixes/Enhancements

- Reduced CPU usage by optimizing file scan algorithm.
- Reduced error log messages when file scan processing queue is full.
- Fixed memory leak when disconnected from the Cisco Cloud.
- Improved handling of file activity from system processes like Spotlight.

AMP for Endpoints Console 5.4.20190430

New

- Changed IP List types to Blocked and Allowed lists.

Bugfixes/Enhancements

- Fixed a bug to improve load times on the AV Definition Summary page.

25 April 2019

AMP for Endpoints Linux Connector 1.10.2

Bugfixes/Enhancements

- Reduced CPU usage by optimizing file scan algorithm.
- Reduced error log messages when file scan processing queue is full.
- Fixed memory leak when disconnected from the Cisco Cloud.

17 April 2019

AMP for Endpoints Console 5.4.20190417

New

- You can now view and configure quarterly reports in addition to monthly and weekly reports. Quarterly reports aggregation is based on calendar quarters.
  - The first default (System-defined) quarterly report will be available in July 2019.
  - Threat Severity graphs won't be available until July 2019 because the feature needs to collect a quarter's worth of data.

17 April 2019

AMP for Endpoints Mac Connector 1.10.1

New

- Added RARv5 archive extraction support.

Bugfixes/Enhancements

- Updated ClamAV to 0.101.2, including changes related to these vulnerabilities:
  - CVE-2019-1787
  - CVE-2019-1788
  - CVE-2019-1789
- Delete stale ClamAV temporary files when file scan terminates abnormally (CSCvo74969).
- Fixed incompatibility with macOS 10.14.3 audit policy changes.
- Fix intermittent file scan failure if debug logging has been enabled for a long time.

AMP for Endpoints Linux Connector 1.10.1

New

- Added RARv5 archive extraction support.

Bugfixes/Enhancements

- Updated ClamAV to 0.101.2, including changes related to these vulnerabilities:
  - CVE-2019-1787
  - CVE-2019-1788
  - CVE-2019-1789
- Delete stale ClamAV temporary files when file scan terminates abnormally (CSCvo74969).
- Fix intermittent file scan failure if debug logging has been enabled for a long time.

2 April 2019

AMP for Endpoints Console 5.4.20190402

New

- Leaving the “Event Type” field blank in the event stream API will now stream all Event Types.

26 March 2019

AMP for Endpoints Linux Connector 1.10.0

New

- Connector now runs ClamAV file scans using an unprivileged process. A new cisco-amp-scan-svc user will be created by the installer.
- Added CLI command /opt/cisco/amp/bin/ampcli defupdate to initiate ClamAV definition update.
- Connector now reports a fault when filesystem monitor or network monitor fails to start (CSCvm10710).

Bugfixes/Enhancements

- Fixed scheduled full scan incorrectly processed as single file scan (CSCvn36511).
- Fixed memory leak when updating cached mount table (CSCvo35582).
- Fixed issue where CPU usage may remain high even after stopping AMP service.
- Fixed RedirFS-related kernel panics (CSCvj44170, CSCvo74991).
- Fixed incorrect exclusion on devtmpfs from on-access scan.
- Fixed Connector status may be stuck at " Offline" after system time change.
- Fixed unintended quarantine when a retro quarantine request is received in Audit mode.
- Update third-party libraries, including changes related to these vulnerabilities:
  - Curl:
    - CVE-2018-16840
  - CiscoSSL:
    - CVE-2018-0732
    - CVE-2018-0737
    - CVE-2018-5407
  - SQLite:

- CVE-2018-20346

IMPORTANT! We recommend that you reboot RHEL/CentOS 6.x computers after upgrading so that the updated RedirFS kernel module can be loaded. The Connector will not force the computer to reboot but the computer will remain susceptible to the defects that can cause kernel panic (CSCvj44170, CSCvo74991) until after reboot.

AMP for Endpoints Mac Connector 1.10.0

New

- Connector now runs ClamAV file scans using an unprivileged process. A new cisco-amp-scan-svc user will be created by the installer.
- Enabled PCRE definitions in ClamAV.
- Added menu item and CLI command /opt/cisco/amp/ampcli defupdate to initiate ClamAV definition update.

Bugfixes/Enhancements

- Fixed scheduled full scan incorrectly processed as single file scan (CSCvn36511).
- Fixed Connector status may be stuck at " Offline" after system time change.
- Fixed unintended quarantine when a retro quarantine request is received in Audit mode.
- Reduced overhead on system, especially when compiling software.
- Fixed memory leak when reading certificates from config.
- Fixed missing log messages for file-op command line logging.
- Updated third-party libraries, including changes related to these vulnerabilities:
  - Curl:
    - CVE-2018-16840
  - CiscoSSL:
    - CVE-2018-0732
    - CVE-2018-0737
    - CVE-2018-5407

19 March 2019

AMP for Endpoints Console 5.4.20190319

New

- There is now a link to the release notes in the console's help.
- The following events are now hidden to reduce the number of extraneous events visible to the user.
  - Quarantine Item Deleted
  - Failed to Delete from Quarantine
  - Attempting Quarantine Delete
- Users can now mute selected compromise artifacts and event types organization-wide to reduce the amount of information that needs to be reviewed in the console.

Bugfixes/Enhancements

- Threat severity information will now be visible in monthly reports generated from April 1, 2019 and on.

5 March 2019

AMP for Endpoints Console 5.4.20190305

New

- Users can now select which types of announcements to receive through email notifications by clicking the **Announcement Email Preferences** link.

Bugfixes/Enhancements

- The date picker on the Policies page for configuring update windows and the filter on the Audit Log page has been updated with a calendar-style interface.
- Email announcements now arrive more quickly after subscribing.

21 February 2019

AMP for Endpoints Windows Connector 6.2.19

New

- This release contains all fixes up to and including 6.2.9 in addition to an experimental engine that inspects and acts on URL telemetry. There are potential compatibility issues with other security products. As such, the engine is configured to be disabled by default. Please contact Cisco TAC for more information.

20 February 2019

AMP for Endpoints Console 5.4.20190220

New

- A summary of metrics is now displayed at the top of the Computers page.
- You can now filter the computer list by operating system by selecting the respective tab on the Computers page.

Bugfixes/Enhancements

- When sending a file for analysis, the first choice on the drop-down list is now the operating system of the default VM selected on the Business page (CSCvn82732).

19 February 2019

AMP for Endpoints Windows Connector 6.2.9

Bugfixes/Enhancements

- Addressed an issue where the Connector could cause Blue Screen of Death (BSOD) under rare conditions (CSCvo24869).
- Improved evaluation of System Process Protection (SPP) event notifications.

5 February 2019

AMP for Endpoints Console 5.4.20190205

Bugfixes/Enhancements

- The navigator in Device Trajectory can now be collapsed and expanded.
- Improved compatibility of the default Exploit Prevention engine configuration with Microsoft Office 365.
- When creating diagnostics for iOS devices, iOS-specific options now appear in the dialog.
- Events page now shows the correct time range type in the filter when redirected from Overview.
- On the Inbox page, clicking the Reset button now correctly sets the time period to the default.

29 January 2019

AMP for Endpoints Windows Connector 6.2.5 (Superseded by 6.2.9)

Bugfixes/Enhancements

- Addressed System Process Protection (SPP) event notification issue which was being triggered under certain conditions, even if the SHA-256 is allow listed (CSCvn41948).
- Improved hash calculation process to prevent deadlock under certain conditions (CSCvn99024).
- Fixed System Process Protection (SPP) exclusions issue which was triggering event notifications for certain processes, even if they are excluded via process exclusion (CSCvn30222).
- Improved evaluation of System Process Protection (SPP) event notifications.
- Fixed issue in Malicious Activity Protection (MAP) engine which caused the computer to freeze or crash after starting Visual Studio in debug mode (CSCvn52070).
- Improved Exploit Prevention engine to prevent deadlock during initialization in rare cases.
- Resolved Exploit Prevention engine compatibility issue with the below applications:
  - Skype Meetings App
  - IPFX plug-in for Outlook
  - MS PowerPoint Presentations (CSCvn69111)
  - Litera ChangePro add-on for Outlook
  - RDP (RD web access)
  - Eden add-on for Outlook (CSCvg00086)
  - Trend Micro

24 January 2019

Cisco Security Connector 1.4.0

Bugfixes/Enhancements

- Improved visibility with TOR browsers in active block mode.

22 January 2019

AMP for Endpoints Console 5.4.20190122

New

- New Device Trajectory interface with navigator for quickly pinpointing events. Non-SHA-256 searches will return results in the legacy Device Trajectory interface.

Bugfixes/Enhancements

- In the Overview tab, if there is no compromise data available yet, the page will display a high level cloud query count.

8 January 2019

AMP for Endpoints Console 5.4.20190108

New

- When editing Windows exclusion sets, there is now a check box to apply the wildcard exclusion to all drive letters.
- It is now possible to opt out of Cisco Maintained Windows and Mac Default Exclusions (at the risk of negatively impacting performance).
- In the Overview tab, users can click individual items in each section to navigate directly to relevant pages in the console.

Bugfixes/Enhancements

- Specified paths in process exclusions for Windows may no longer end in a path separator (backslash).

Release note links

Current release notes can be found here.

Other release notes can be found at the following links:

- 2020 release notes
- 2018 release notes
- 2017 release notes
- 2016 release notes
- 2015 release notes
- 2014 release notes
- 2013 release notes