AMP for Endpoints User Guide

Last Updated: October 31, 2017

Table of Contents

CHAPTER 1
DASHBOARD

The AMP for Endpoints Dashboard gives you a quick overview of trouble spots on devices in your environment along with updates about malware and network threat detections. From the Dashboard page you can drill down on events to gather more detailed information and remedy potential compromises.

System Requirements

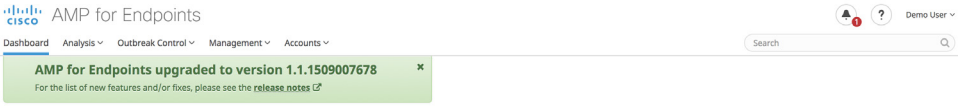
To access the AMP for Endpoints Console, you will need one of the following Web browsers:

- Microsoft Internet Explorer 10 or higher
- Mozilla Firefox 14 or higher
- Apple Safari 6 or higher
- Google Chrome 20 or higher

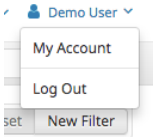
Menu

The menu bar at the top indicates the total number of installs and the number of malware detections in the last 7 days. The current number of system announcements is also shown at the top of the page along with a link to view previous announcements. You can also choose to receive announcements via email from the announcements page or your account page. Menu items take you to the Dashboard, Analysis, Outbreak Control, Reports, Management, and

Accounts, as indicated below. It also has a link to the Help system, Language selector, and User (displayed as the currently logged-in user's name).



The User link opens a menu containing **My Account** and **Log Out** links. The **My Account** link will take you directly to the Users page for your account so you can make changes, and the **Log Out** link ends your session.



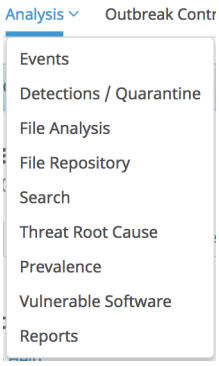
You can perform a Search from any page using the search box in the menu bar. There is also a global group filter to present a more granular view on the **Dashboard Overview** and **Heat Map** tabs and the Threat Root Cause and Deployment Summary pages.

Dashboard

The **Dashboard** link takes you back to the Dashboard, which contains different widgets that highlight events in your environment that require attention.

Analysis

The **Analysis** menu contains the following items related to analysis of threats in your environment:



- The Events Tab to view raw events from Connectors.
- The Detections / Quarantine to view any detections and items that were quarantined.

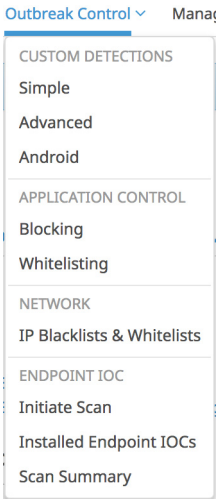
- Cognitive Incidents, which takes you to an Events view filtered to show all cognitive threat Indications of Compromise in your business. You must have Cognitive Threat Analytics enabled on the Business page to see this menu entry.
- Agentless Cognitive Incidents shows incidents associated with computers that do not have an AMP for Endpoints Connector installed. You must have Cognitive Threat Analytics enabled on the Business page to see this menu entry.
- File Analysis explains what a binary does in detail.
- File Repository downloads files retrieved from your AMP for Endpoints Connectors (Administrator only).
- Click Search to find data from your AMP for Endpoints deployment.

> **TIP!** You can also access the search function from the menu bar on any page.

- Threat Root Cause shows how malware is getting onto your computers.
- Prevalence allows you to view files that have been executed in your deployment.
- Select Vulnerable Software to view applications with known vulnerabilities observed by the AMP for Endpoints Connector.
- Click on Reports to see weekly reports about your AMP for Endpoints deployment.

Outbreak Control

The **Outbreak Control** menu contains items related to controlling outbreaks in your network:

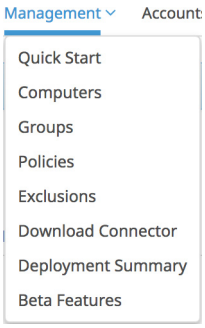


- Custom Detections
  - Simple to convict files that are not yet classified.
  - Advanced to create signatures that will detect parts of the Portable Executable (PE) file.
  - Android to warn of new threats or unwanted apps.
- Application Control

  - Blocking to stop executables from running.
  - Whitelisting to create lists of applications that will not be wrongly detected.
- Network
  - IP Blacklists & Whitelists allow you to explicitly detect or allow connections to specified IP addresses.
- Endpoint IOC
  - Initiate Scan to schedule and start IOC scans on your AMP for Endpoints Connectors (Administrator only).
  - Installed Endpoint IOCs to upload new endpoint IOCs and view installed endpoint IOCs (Administrator only).
  - Scan Summary to view the results of endpoint IOC scans.

Management

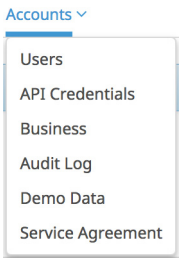
The **Management** menu contains items that allow you to manage your AMP for Endpoints Connectors, as follows.



- Quick Start to access the AMP for Endpoints first use wizard (administrator only).
- Computers to display all the computers in this account.
- Groups to organize computers into groups.
- Policies to view and modify Connector configuration.
- Exclusions to exclude directories, extensions, and threats from being detected.
- Download Connector to create Connector installers.
- Deployment Summary to view deployment failures.

Accounts

The **Accounts** menu contains items related to AMP for Endpoints Console accounts, as follows:

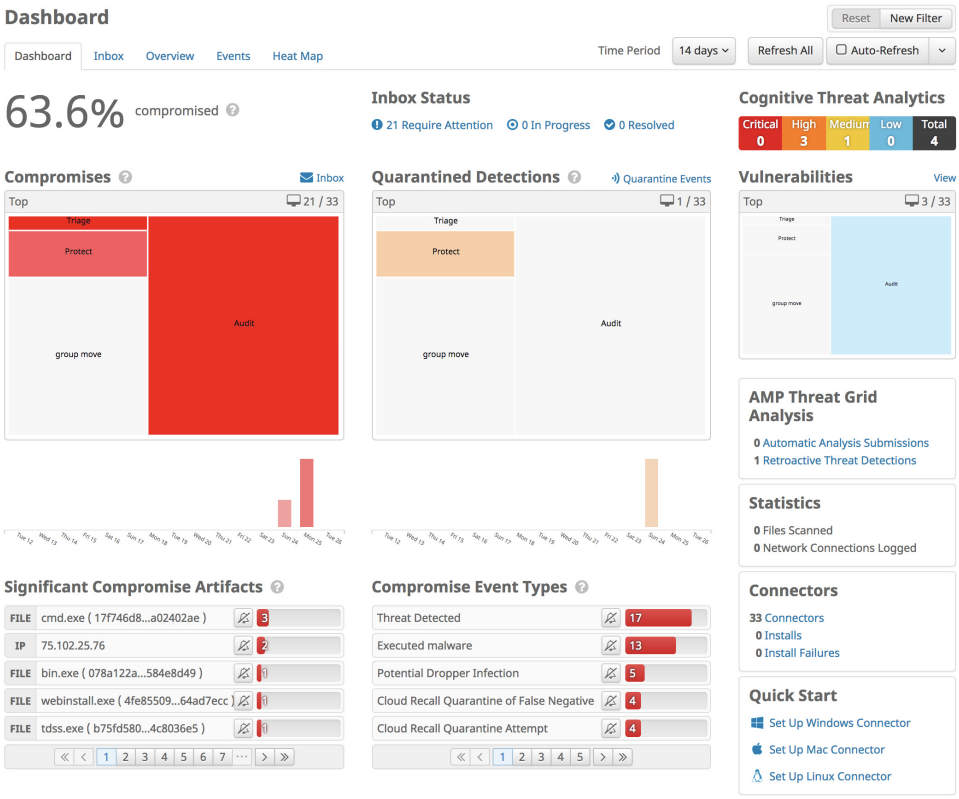


- Users to view and create users. (Administrator only. My Account for unprivileged users.)
- API Credentials to set up 3rd party application access via the AMP for Endpoints API.
- Business to set the company name, default group and default policy, and view license information (administrator only).
- Audit Log to see changes to your account (administrator only).
- Demo Data to populate your Console with sample events (administrator only).
- Applications to view settings of applications you have authorized to receive events from your AMP for Endpoints deployment. This item is only visible if applications have been authorized (administrator only).
- **Service Agreement** displays the AMP for Endpoints products subscription agreement.

Dashboard Tab

The **Dashboard** tab offers a view of threat activity in your organization over the past 14 days, as well as the percentage of compromised computers and the status of items in your Inbox Tab.

You can create, edit, or reset any Filters for the Dashboard and Inbox tab views. The **Time Period** selection applies to all the data in the **Dashboard** tab.



You can click the **Refresh All** button to load the most current data on the page or set an interval for the data to reload automatically by clicking the **Auto-Refresh** button. Select a time interval of 5, 10, or 15 minutes for the data to be loaded. When the Auto-Refresh is active, a check mark will be present on the button. To stop the page from refreshing, click the check mark to clear it.

In addition to heat map views for Compromises, Quarantined Detections, and Vulnerabilities, you can also find a summary of other information including:

- Cognitive Threats in your environment, if you have configured it in the Features for your business.
- Automated submissions and retroactive threat detections through AMP Threat Grid, if you have configured Automatic Analysis of Low Prevalence Executables.
- Statistics on the number of files scanned and network connections logged by your AMP for Endpoints Connectors.

> **IMPORTANT!** Network connection logging requires **Device Flow Correlation** to be enabled in your Policies.

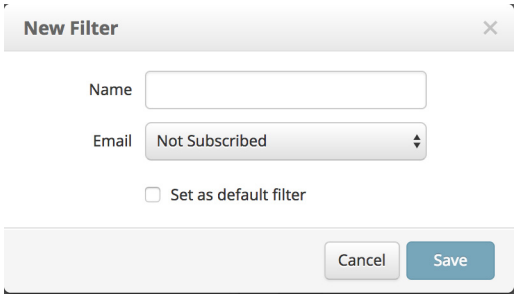
- A summary of active Connectors, Connector installs, and install failures.
- Links to the **Quick Start** setup for each Connector type.

Filters

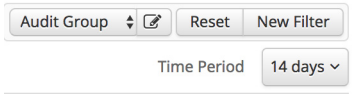
You can filter activity by designated group, time period (the past 14 days, 7 days, 1 day, or 1 hour), date/time selection, compromise-specific artifacts and compromise event types.

Each of these filters may be applied alone or as a combination of filters. Compromise artifacts and compromise event type filters apply only to compromise-related information. Any of the page filters applied here will also apply to the Inbox tab.

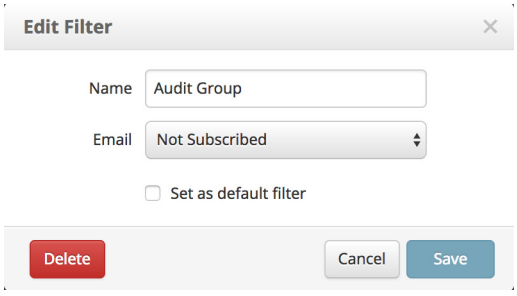
Select groups, artifacts, event types and the time period you want to see then click New Filter to create a custom filter. You can assign a name to the filter, select whether to receive immediate, hourly, daily, or weekly email alerts, and set the filter as the default view of your Dashboard and Inbox tabs.



Once you have saved a custom filter you can select it from the drop down, edit the selected filter, or reset the view to the default with no filters applied.



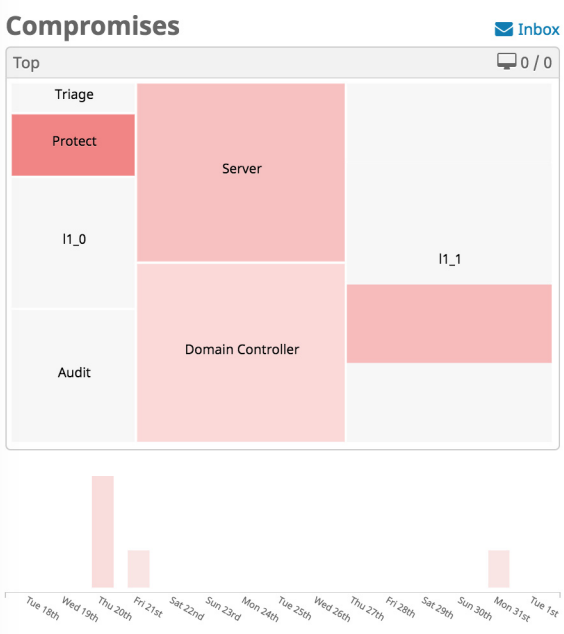
Use the edit button next to the filter name to modify or delete the selected filter.



Compromises

By definition, compromises represent potentially malicious activity that has been detected by AMP that has not been quarantined but that may require action on your part. Compromises are

displayed through a heat map showing groups with compromised computers and a time graph showing the number of compromises for each day or hour over the past 14 days. Click the **Inbox** link to view the compromises on the Inbox Tab and take steps to resolve them.

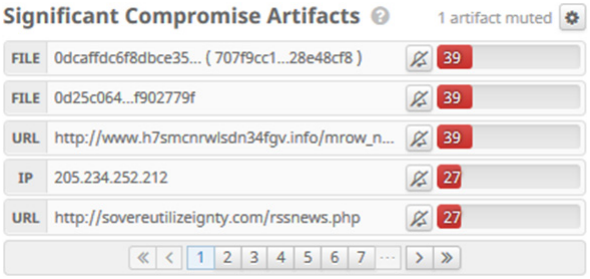


Click on a group in the heat map to drill down into that group and show child groups. You can also drill down by date/time, compromise artifact, and/or compromise event type. Drilling down will also change the view of the rest of the items on the **Dashboard** tab, including the Quarantined Detections and Vulnerabilities heat maps. Click on one of the bars in the time graph to filter the dashboard view to the specific day that the selected compromises occurred. Note that selecting a custom time period by doing this “grays out” and disables the Auto-Refresh button. Click the **Reset** button or select a time period from the drop down menu to re-enable the Auto-Refresh button.

IMPORTANT! There can be more compromise events than computers compromised in a time period if the same computers were compromised more than once.

Significant Compromise Artifacts

Compromise Artifacts are files, IP addresses or URLs associated with compromises in the specified time period. The top 100 most significant compromise artifacts are listed in order of prevalence.



Click on a compromise artifact to filter compromise-related data on the Dashboard and Inbox view by the selected artifact. If you do not want the Dashboard or Inbox to reflect compromise-related data associated with a particular artifact, you can mute the artifact type by clicking on the bell icon.

You can also manage the muted artifacts by clicking on the cog icon. Unmute the artifact by clicking on the bell icon. Muting of artifacts will only affect the user account for which the change was made. It will not affect other user accounts.

Once you mute an artifact, it will not appear in the Significant Compromise Artifacts list. It will also not be included in the compromise-related data that appears on the Dashboard or the Inbox. If you mute an artifact, it will remain muted until you unmute it using the cog icon. Muting will carry over to subsequent visits to the Dashboard or Inbox.

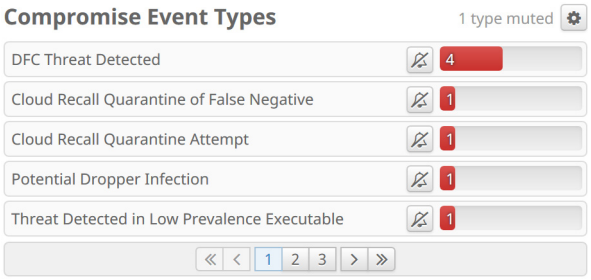
You can view information about a detected artifact by clicking on an artifact. Selecting an artifact will exclude data for all other artifacts in the % compromised, Compromises, and Compromise Event Types.

As long as an artifact is selected, only that artifact will be applied to the page. You can deselect the selected artifact by clicking on the blue X on the upper right-hand side of the Significant Compromise Artifacts box.

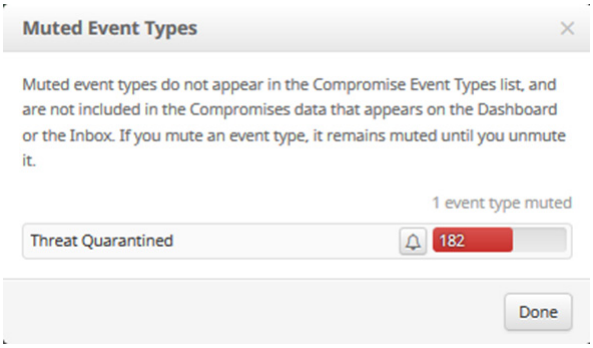
Compromise Event Types

Compromise event types describe events that AMP for Endpoints has detected. They include file, network, and Connector activity. The **Compromise Event Types** feature shows the number of each type of event that has been detected within the designated time period (such as 1 hour, 1 day, 7 days, or 14 days). You can click on a compromise event type to filter the compromise-related data on the Dashboard by the selected event type.

If you do not want to receive notification of a particular event type, or do not want the Dashboard or Inbox to reflect that event type, you can mute the event type by clicking on the bell icon.

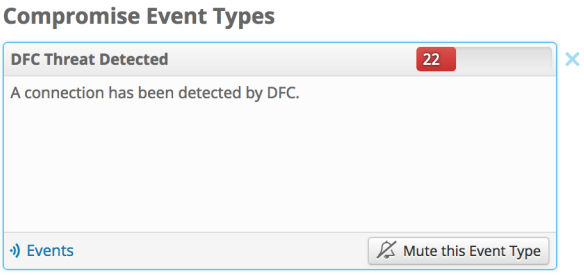


You can also view the event types that are muted by clicking on the cog icon. Unmute the event type by clicking on the bell icon. If you mute or unmute an event type, that change will only affect the user account for which the change was made. It will not affect other user accounts.



Once you mute an event, it will not appear in the **Compromise Event Types** list. It will also not be included in the compromises data that appears on the Dashboard or the Inbox. If you mute an event, it will remain muted until you unmute it using the cog icon. Muting will carry over to subsequent visits to the Dashboard or Inbox.

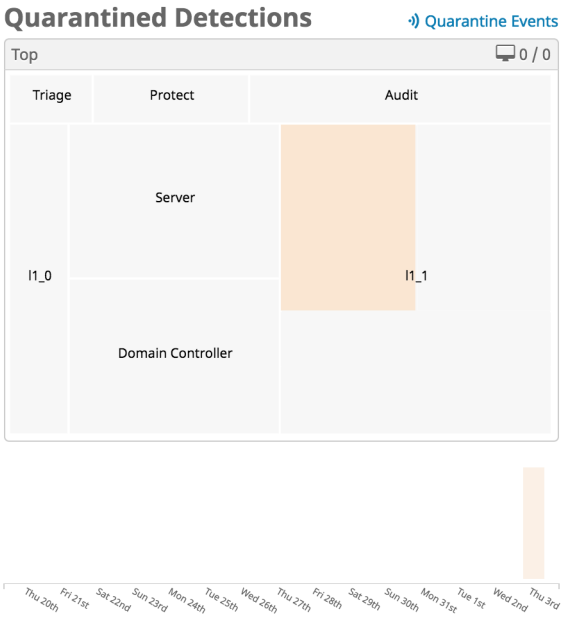
You can view information about a detected event type by clicking on the event type name. Selecting a compromise event type will exclude data for all other event types in **% compromised, Compromises**, and **Compromise Artifacts** while that event type is selected.



As long as a compromise event type is selected, only that event type will be applied to the page. You can deselect the selected event type by clicking on the blue X on the upper right-hand side of the **Compromise Event Types** box.

Quarantined Detections

Quarantined detections are potential compromises or malicious events that were detected and successfully quarantined, and so do not require any attention by the user. They are depicted through a heat map showing groups with computers on which malicious activity was detected, as well as a time graph showing the number of quarantines during the selected period.

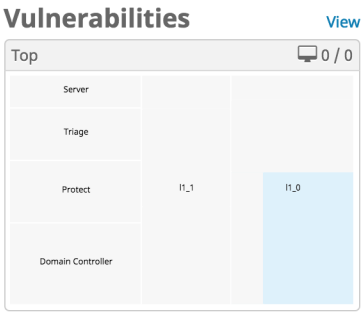


Click on a group in the heat map to drill down into that group and show child groups. Drilling down will filter the data that appears on the Dashboard tab - including the Compromises and Vulnerabilities heat maps - to show the selected groups or child groups.

Clicking the bars in the time graph will filter the dashboard view to the specific date and time (from 14-day to two-minute increments) on which the selected quarantines occurred. You can also click the **Quarantine Events** link to see a filtered view of the Events Tab showing all quarantines.

Vulnerabilities

Vulnerabilities are displayed through a heat map that shows groups that include computers with known vulnerable applications installed.

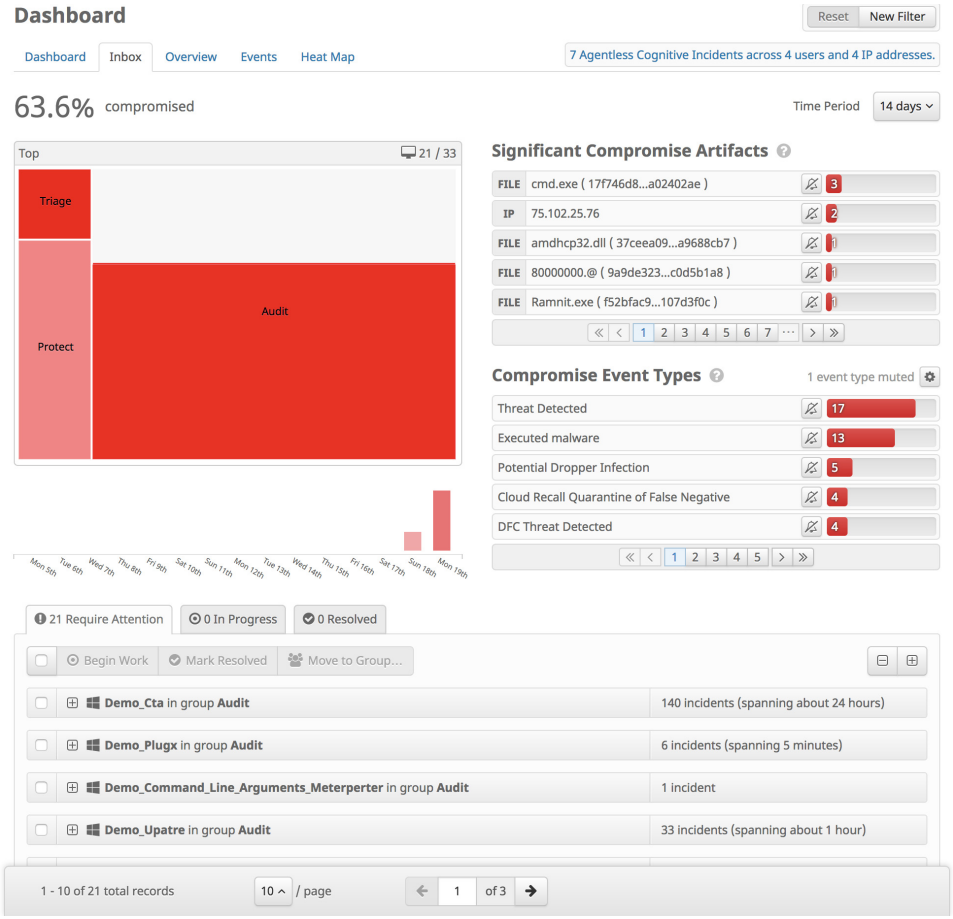


Click on a group in the heat map to drill down into that group and show child groups. Drilling down will also filter the data that appears on the Dashboard tab - including the Compromises and Quarantined Detections heat maps - to show the selected groups or child groups. Click the **View** button to go to the Vulnerable Software page.

Inbox Tab

The **Inbox** is a tool that allows you see compromised computers in your business and track the status of compromises that require manual intervention to resolve. You can filter computers to work on by selecting Groups in the heat map, selecting a day with compromises in the bar chart, selecting a SHA-256 from the Significant Compromise Artifacts list, or selecting from the Compromise Event Types list. These Filters can be saved and set as your default view. You can also filter the computer list by those that require attention, those that are in progress, and

those that have been resolved. When a computer is marked as resolved, it is no longer reflected in data on the Dashboard or Inbox.



IMPORTANT! Items in your inbox are retained for 14 days. You will not be able to see any compromises older than 14 days regardless of their status.

The Compromise Event Types feature shows the number of each type of event that has been detected within the designated time period (such as 1 hour, 1 day, 7 days, or 14 days). If you do not want to receive notification of a particular event type, you can mute the event type by clicking on the bell or the cog icon.

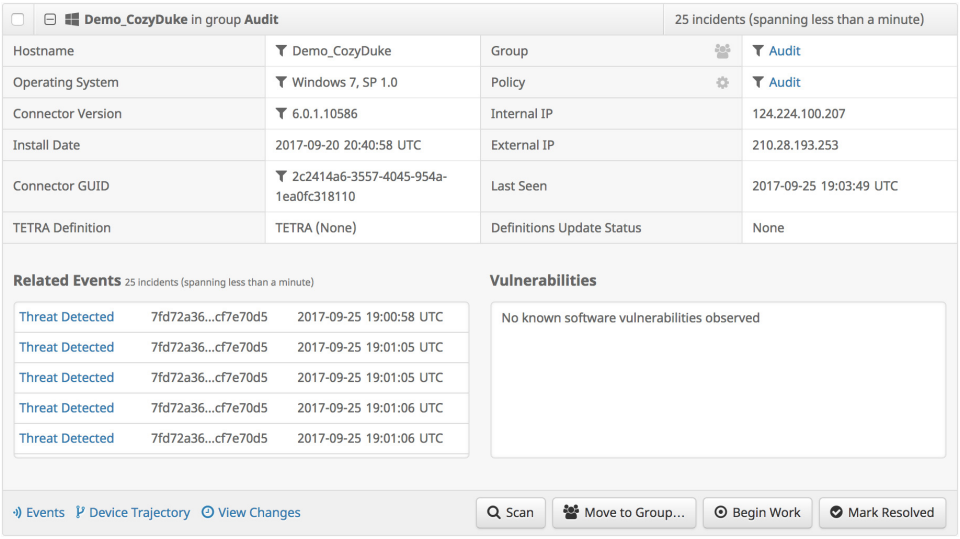
If you have **Cognitive Threat Analytics** enabled from the Business page you will also see the number of agentless cognitive incidents across your organization. Click on this link to view a list of devices and incidents on the Agentless Cognitive Incidents page.

IMPORTANT! If your inbox is filtered by Significant Compromise Artifacts and you click **Mark Resolved** for multiple computers, any computers with more than one artifact will not be resolved. You must resolve those computers individually as multiple artifacts indicate more than one source of compromise.

You can select one or more computers to begin work on, mark as resolved, or move to different Groups. You can also select multiple computers with an **In Progress** status and click the **Focus** button to only see those computers in the list. Click **Show All** to see the complete list again.

In some cases, a computer may have been compromised but never marked as resolved and is no longer visible in your Inbox because the compromise is older than two weeks. If that computer is compromised again, an icon will appear next to the computer in your Inbox to indicate that a previous compromise that was never marked as resolved also exists. You will need to check the Device Trajectory and Events for that Connector to find any previous compromise events and ensure they have been resolved.

Expand the entry for a compromised computer to display basic information about that computer along with a list of events related to the compromise and any Vulnerable Software detected on the computer. You can also perform numerous actions on the computer from here, such as: running a full or flash scan, moving the computer to a different group, viewing the device trajectory for the computer. and marking the compromise as resolved. If you move a computer to a new group, compromise data associated with that computer will appear in the data for the new group.



Click the name of a related event to launch Device Trajectory for the computer focused on that event. Click the SHA-256 of a related event to view all the computers in your business that also have compromise events involving that SHA-256.

To determine the extent of the compromise to a computer and help resolve the incident you can:

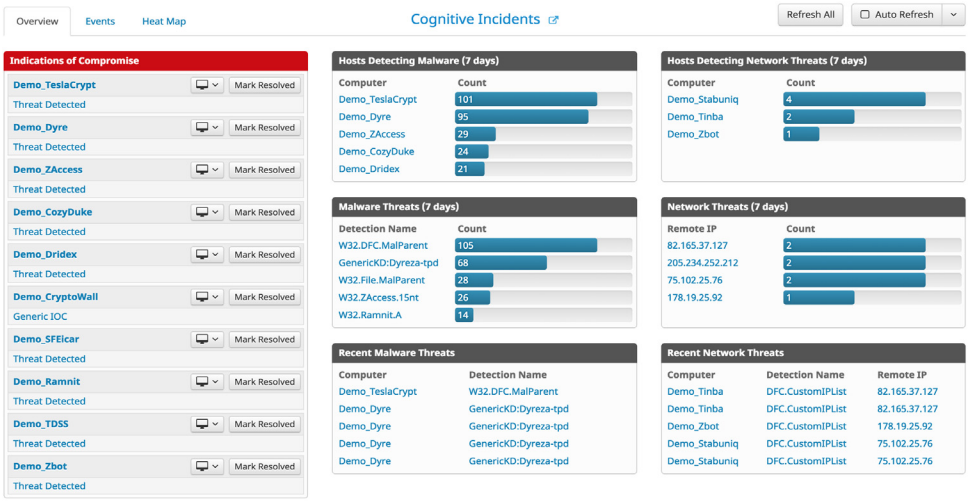
- Open the Events Tab filtered to the specific computer
- Launch Device Trajectory for the computer
- Click View Changes to see the Audit Log for that computer
- Launch a file scan or Endpoint IOC Scanner

To track and manage the status of a compromised computer, click on **Begin Work** to begin resolving the compromise on the selected computer. Once you have begun work, the status of the computer will change to **In Progress**. You can click on **Mark Resolved** when the work is completed.

For more details on how to use AMP for Endpoints to resolve incidents see Cisco AMP for Endpoints Demo Data Stories.

Overview Tab

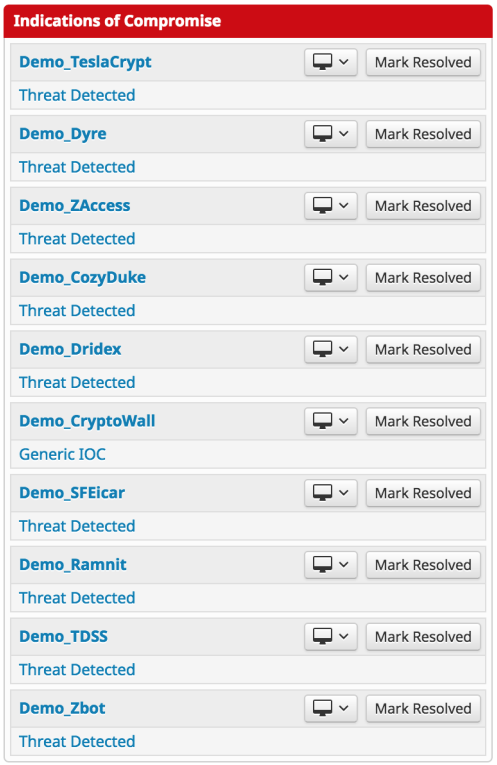
The **Overview** tab is composed of multiple widgets that highlight recent malicious activity in your AMP for Endpoints deployment. The tab is divided into three types of information: indications of compromise (IOC), malware detections, and network threats.



You can click the **Refresh All** button to load the most current data on the page or set an interval for the data to reload automatically by clicking the **Auto-Refresh** button. Select a time interval of 5, 10, or 15 minutes for the data to be loaded. When the Auto-Refresh is active, a check mark will be present on the button. To stop the page from refreshing, click the check mark to clear it.

Indications of Compromise

The **Indications of Compromise** widget provides you with a list of potentially compromised devices in your AMP for Endpoints deployment and quick links to inspect activity to remedy the problem. After the issue has been addressed, you can then mark it as resolved.

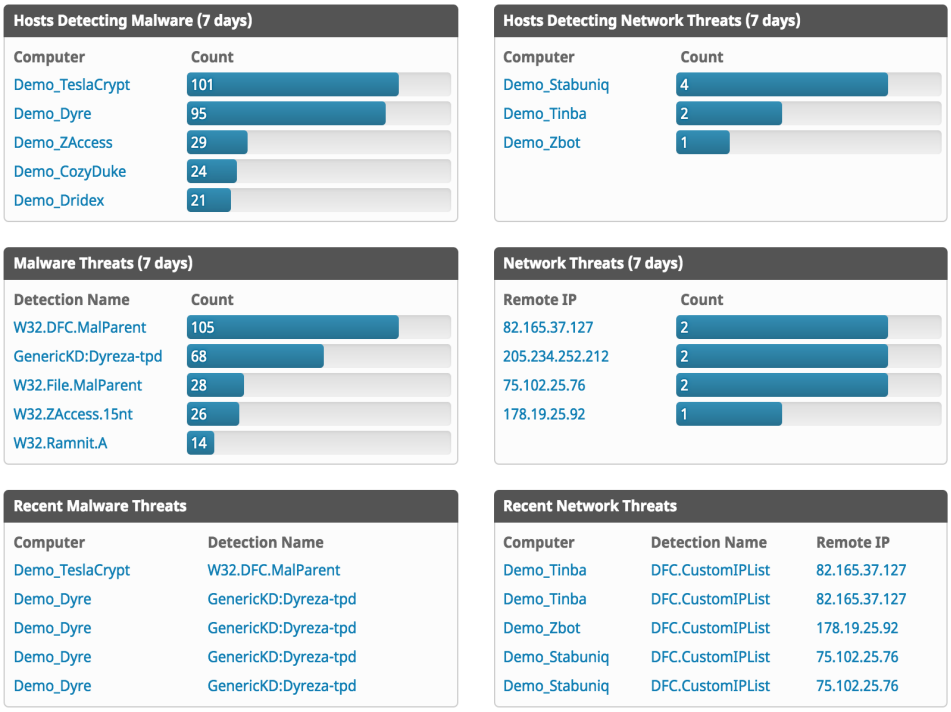


AMP for Endpoints calculates devices with Indications of Compromise based on events observed over the last 7 days. Events such as malicious file detections, a parent file repeatedly downloading a malicious file (potential dropper infection), or multiple parent files downloading malicious files (multiple infected files) are all contributing factors. Devices considered to be at the highest risk are displayed at the top of the list.

You can click on the name of a device in the list to view the most recent events observed or click the information menu to launch Device Trajectory or Computer Management. Clicking on the name of the indication of compromise will take you to the Device Trajectory for the computer focused on the events that make up the indication of compromise. For indication of compromise descriptions, please see Threat Descriptions.

Malware and Network Threat Detections

The most recent threats detected in your AMP for Endpoints installation are displayed, along with the top threats over the last 7 days, and the hosts detecting the most threats over the last 7 days.



Clicking on a detection name or remote IP address will bring you to the **Events** tab for that detection. Clicking on a computer name will bring you to the **Events** tab for that computer.

IMPORTANT! For descriptions of threat names, see AMP Naming Conventions.

Events Tab

The **Events** tab initially shows the most recent events in your AMP for Endpoints deployment. Navigating to the **Events** tab by clicking on a threat, IP address, or computer name in the **Dashboard** tab will provide different filtered views.

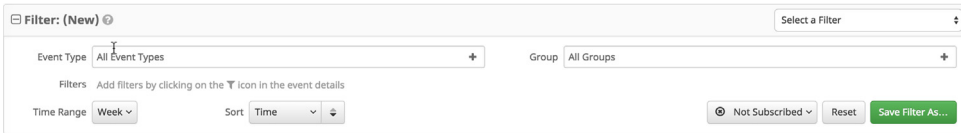
Filters and Subscriptions

Filters are shown at the top of the **Events** tab. You can select a previously saved filter from the drop-down on the right side or add event types, groups, or specific filters from existing events. To remove a filter criteria, click the **x** next to the item you want to remove. You can also sort the Events list in ascending or descending order based on criteria from the drop-down list.

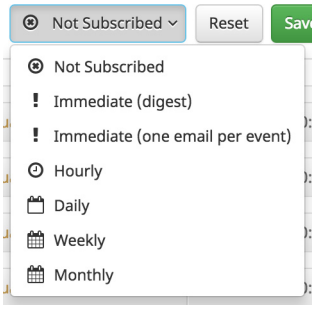
Click the **Reset** button to remove all filter criteria or click the **Save Filter As** button to save the current filtered view.

IMPORTANT! The **Time Range** filter is set to one week by default if you have less than 10,000 Connectors deployed. If you have more than 10,000 Connectors deployed it will be set to one day.

When viewing a saved filter, you can update the filter and click **Save New** to save the changes as a new filter or click **Update** to overwrite the existing filter.



To subscribe to a filter view click the **Not Subscribed** button to show a menu with subscription timing options. You can subscribe to events with immediate, hourly, daily, weekly, or monthly notifications. There are options to receive immediate alerts as one email per event, or a single email digest containing 5 minutes of events.

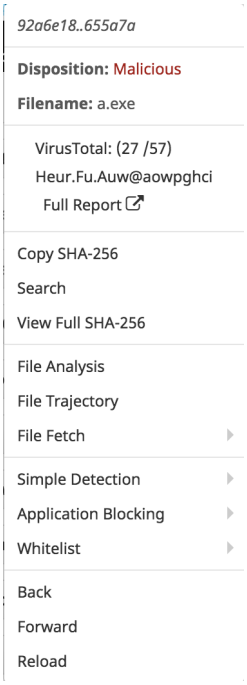


Once you have selected the notification frequency click **Update** to save your settings. If you no longer want to receive notifications for a filter view, switch the notification frequency to **Not Subscribed** and click **Update**.

SHA-256 File Info Context Menu

Right-clicking on a SHA-256 in the AMP for Endpoints Console will display a specific context menu that allows you to see additional information and perform several actions. The context menu displays the current disposition of the SHA-256 as well as the specific filename

associated with it. You can also see how many vendors detect the file according to VirusTotal. The longest common name used for the file on VirusTotal is also displayed.



You can copy or view the full SHA-256 value or perform a search for that SHA-256 to see where else it was seen in your organization. You can also launch File Trajectory for the SHA-256, submit it for File Analysis, or fetch it for the File Repository. The context menu also allows you to quickly add the SHA-256 to one of your outbreak control lists. Options are available to add it to a new or existing Simple, Blocking, or Whitelisting outbreak control list.

IMPORTANT! Unprivileged users will not have access to all items on the context menu.

List View

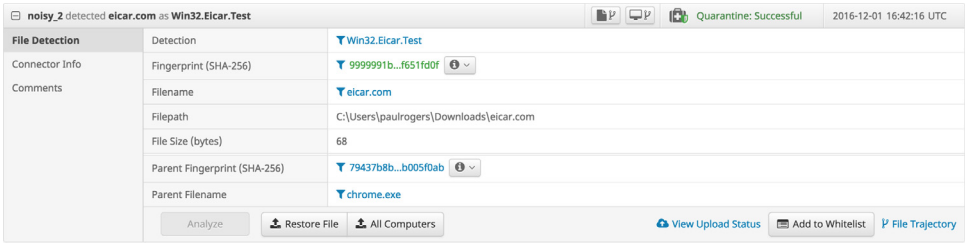
List View initially shows the name of the computer that had a detection, the name of the detection, the most recent action taken, and the time and date of the event. If there were any command line arguments associated with the even they will also be displayed. Click on an event to view more detailed information on the detection, Connector info, and any comments about the event. In the detailed view, you can access context menus through the information icon. The context menu for a computer entry allows you to launch the Device Trajectory for that computer or open the Computer Management page. The context menu for a file entry is the same as the SHA-256 File Info Context Menu. Click the **Analyze** button to retrieve the file and send it for File Analysis. File Repository must be enabled to retrieve the file. If a file was

quarantined, you can choose to restore the file for that computer or for all computers that quarantined it.

IMPORTANT! If the **Analyze** button is not available, it may be that the file has already been submitted, the **File Repository** is not enabled, or the current user is not an administrator.

Click an entry with a filter icon to filter the list view by entries with matching fields. You can also use the **Export to CSV** button to export the current filtered view to a CSV file to download.

IMPORTANT! All dates and times in the exported CSV file will be in UTC regardless of your Time Zone Settings.

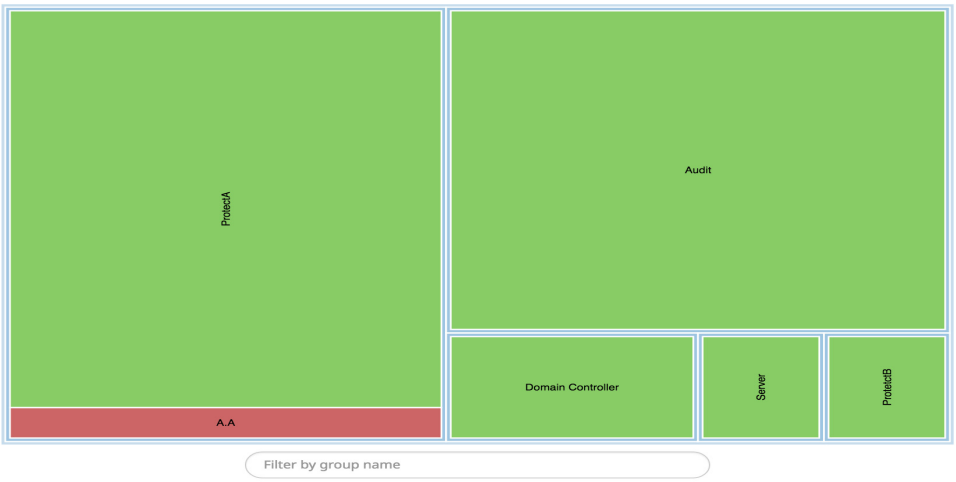


IMPORTANT! For descriptions of threat names, see AMP Naming Conventions.

Heat Map Tab

The **Heat Map** tab shows at a glance which groups require attention. The size of each rectangle is based on the number of computers in the group. The color ranges from green to yellow to red. Green indicates that there have been no detections in that group in the last 7 days. Shades of yellow indicate that there have been some detections, but the ratio between the number of computers and detections is small (that is, the mean detections per computer is < 0.10). Shades

of red indicate that there have been a large number of detections compared to the number of computers in a group (that is, the mean detections per computer is > 0.10).



Clicking a group in the **Heat Map** will take you to a filtered view of the Events Tab showing **Threat Detected** events for that group.

You can search for groups by name in the box at the bottom indicated by **Search the groups in the heat map**. This will white out the other groups and highlight the one you are searching for.

You can hover your pointer over a group and see the number of computers, detections in the last 7 days, and the mean detections per computer. The tree map refreshes hourly, so changes may not always be immediately apparent.

CHAPTER 3
OUTBREAK CONTROL

AMP for Endpoints offers a variety of lists, referred to as **Outbreak Control**, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Application Blocking, Application Whitelists, Advanced Custom Detections, and IP Blacklists and Whitelists. These will be discussed in the sections that follow.

Custom Detections - Simple

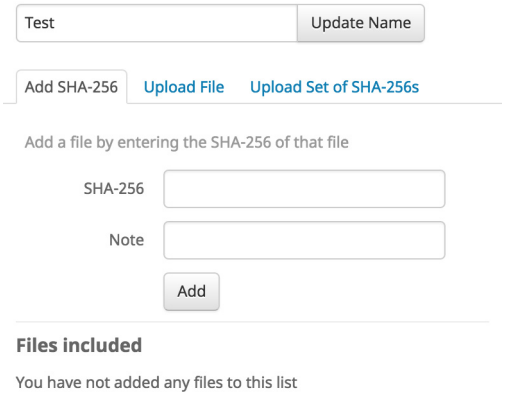
A **Simple Custom Detection** list is similar to a blacklist. These are files that you want to detect and quarantine. Not only will an entry in a Simple Custom Detection list quarantine future files, but through Retrospective it will quarantine instances of the file on any endpoints in your organization that the service has already seen it on.

To create a Simple Custom Detection list, go to **Outbreak Control > Simple**. Click **Create** to create a new Simple Custom Detection, give it a name, and click on **Save**.

After you save the Simple Custom Detection, click on **Edit** and you will see three ways to add values to this list.

You can add a single SHA-256 and create a note about the file. You can upload a file (up to 20MB) and the SHA-256 will be taken from the file and you can add a note. You can also upload a set of SHA-256s. When uploading a set of SHA-256s, they must be contained in a text file with one SHA-256 per line. The SHA-256s and notes can be seen if you click on the **Files**

included link on the bottom right. If you added a SHA-256 that you did not intend to, you can click on **Remove**. You can also edit the name of the list and click **Update Name** to rename it.



Note that when you add a Simple Custom Detection, it is subject to caching. The length of time a file is cached depends on its disposition, as follows:

- Clean files: 7 days
- Unknown files: 1 hour
- Malicious files: 1 hour

If a file is added to a Simple Custom Detection list, the cache time must expire before the detection will take effect. For example, if you add a simple custom detection for an unknown file 5 minutes after it was cached, the detection will not take effect for another 55 minutes.

IMPORTANT! You cannot add any file that is on our global whitelist or is signed by a certificate that we have not revoked. If you have found a file that you think is incorrectly classified, or is signed and want us to revoke the signer, please contact Support.

Click the **View All Changes** link to see the Audit Log with all records filtered to show only Simple Custom Detection entries. Click **View Changes** next to a single Simple Custom Detection list to view the Audit Log with all records filtered to show only the records for that specific detection list.

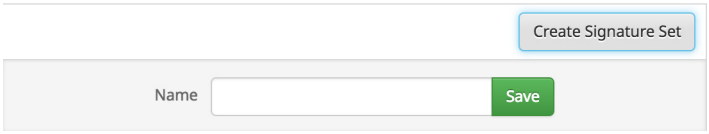
Custom Detections - Advanced

Advanced Custom Detections are like traditional antivirus signatures, but they are written by the user. These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:

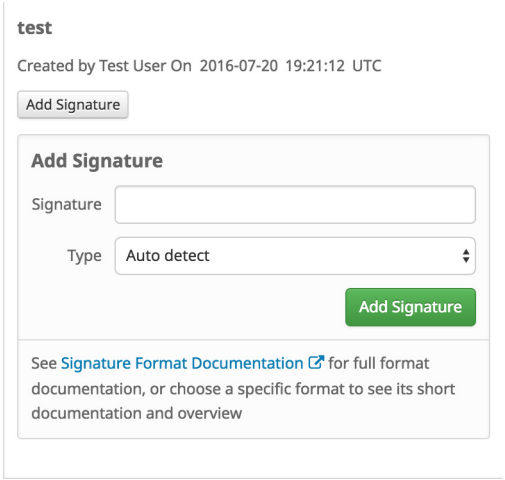
- MD5 signatures
- MD5, PE section-based signatures
- File body-based signatures
- Extended signature format (offsets, wildcards, regular expressions)
- Logical signatures
- Icon signatures

More information on signature formats can be found at http://docs.amp.cisco.com/clamav_signatures.pdf. These signatures are compiled into a file that is downloaded to the endpoint.

In order to create advanced custom detections, go to **Outbreak Control > Advanced**. Click on **Create Signature Set** to create a new Advanced Custom Detection set, give it a name, and click **Create**.



After you create the Advanced Custom Detection set, click on **Edit** and you will see the Add Signature link. Enter the name of your signature and click **Create**.



After all of your signatures are listed, select **Build a Database from Signature Set**. If you accidentally add a signature you did not want, you can delete it by clicking **Remove**.

IMPORTANT! Any time you add or remove a signature you MUST click on **Build a Database from Signature Set**

Note that when you create an advanced custom detection for a file that it is subject to caching. The length of time a file is cached for depends on its disposition as follows:

- Clean files: 7 days
- Unknown files: 1 hour
- Malicious files: 1 hour

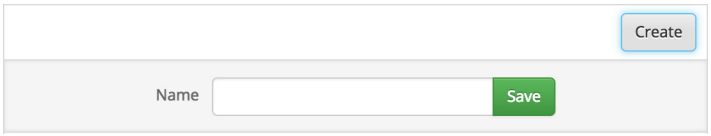
If a file is added to an advanced custom detection set, the cache time must expire before the detection will take effect. For example, if you add an advanced custom detection for an unknown file 5 minutes after it was cached, the detection will not take effect for another 55 minutes.

Click the **View All Changes** link to see the Audit Log with all records filtered to show only Advanced Custom Detection entries. Click **View Changes** next to a single list to view the Audit Log with all records filtered to show only the records for that specific detection list.

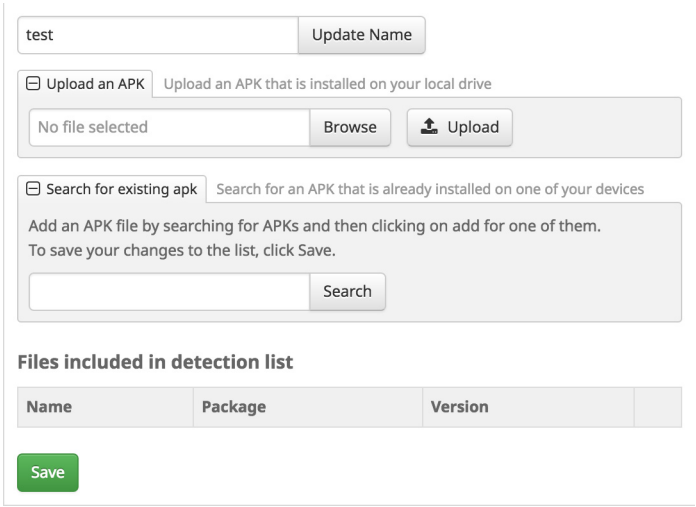
Custom Detections - Android

An **Android Custom Detection** list is similar to a Simple Custom Detection list except that the device user is warned about the unwanted app and must uninstall it themselves. You can add new malicious apps to an Android Custom Detection list as well as apps that you do not want your users installing on their devices.

To create an Android Custom Detection list, go to **Outbreak Control > Android**. Click **Create** to create a new Android Custom Detection, give it a name, and click on **Save**.



After you save the custom detection, click on **Edit** and you will see two ways to add values to this list.



You can add an app by uploading its APK file or by searching through an inventory of all APK files installed on devices running the AMP for Endpoints Android Connector and selecting the ones you want to detect. Once you have finished adding apps to the list, click **Save**.

Click the **View All Changes** link to see the Audit Log with all records filtered to show only Android Custom Detection entries. Click **View Changes** next to a single Android Custom Detection list to view the Audit Log with all records filtered to show only the records for that specific detection list.

Application Control - Blocking

An **application blocking list** is composed of files that you do not want to allow users to execute but do not want to quarantine. You may want to use this for files you are not sure are

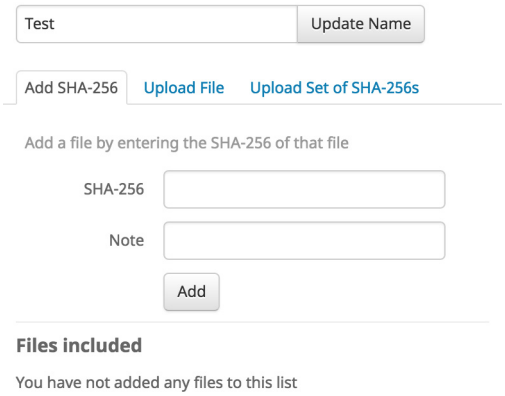
malware, unauthorized applications, or you may want to use this to stop applications with vulnerabilities from executing until a patch has been released.

IMPORTANT! Any SHA-256 value can be added to an application blocking list, but only executable type files will be prevented from opening.

In order to create an application blocking list, go to **Outbreak Control > Blocking**. Click **Create** to create a new application blocking list, give it a name, and click on **Save**.

After you save the application blocking list, click on **Edit** and you will see three ways to add values to this list.

You can add a single SHA-256 and create a note about the file. You can upload a file (up to 20MB) and the SHA-256 will be taken from the file and you can add a note, or you can upload a set of SHA-256s. When uploading a set of SHA-256s they must be contained in a text file with one SHA-256 per line. The SHA-256s and notes can bee seen if you click on the **Files included** link on the bottom right. If you accidentally added a SHA-256 that you did not want to, click **Remove**. You can also edit the name of the list and click **Update Name** to rename it.



Note that when you add a file to an application blocking list that it is subject to caching. If the file is not in your local cache and you have **On Execute Mode** set to **Passive** in your policy it is possible that the first time the file is executed after being placed in your application blocking list it will be allowed to run. Setting On Execute Mode to Active in your policy will prevent this from occurring.

If the file is already in your local cache you will have to wait until the cache expires before application blocking takes effect. The length of time a file is cached for depends on its disposition as follows:

- Clean files: 7 days
- Unknown files: 1 hour
- Malicious files: 1 hour

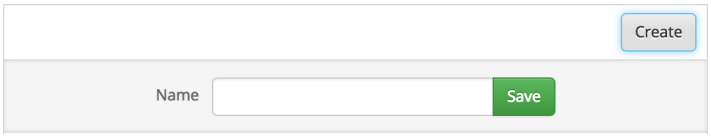
If a file is added to an application blocking list, the cache time must expire before the detection will take effect. For example, if you add an unknown file to a list 5 minutes after it was cached, the detection will not take effect for another 55 minutes.

Click the **View All Changes** link to see the Audit Log with all records filtered to show only application blocking entries. Click **View Changes** next to a single application blocking list to view the Audit Log with all records filtered to show only the records for that specific blocking list.

Application Control - Whitelisting

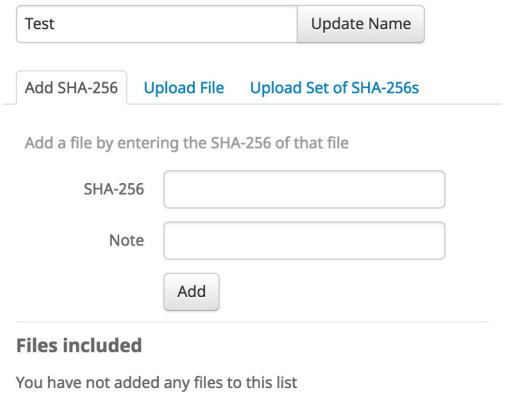
Application whitelists are for files you never want to convict. A few examples of this are a custom application that is detected by a generic engine or a standard image that you use throughout the company.

To create an application whitelist, go to **Outbreak Control > Whitelists**. Next click **Create** to create a new whitelist, give it a name, and click **Save**.



After you save the whitelist, click **Edit** and you will see three ways to add values to this list.

You can add a single SHA-256 and create a note about the file. You can upload a file (up to 20MB) and the SHA-256 will be taken from the file and you can add a note, or you can upload a set of SHA-256s. When uploading a set of SHA-256s, they must be contained in a text file with one SHA-256 per line. The SHA-256s and notes can bee seen if you click on the **Files included** link on the bottom right. If you added a SHA-256 that you did not want to, click **Remove**. You can also edit the name of the list and click **Update Name** to rename it.



Click the **View All Changes** link to see the Audit Log with all records filtered to show only application whitelist entries. Click **View Changes** next to a single application whitelist to view the Audit Log with all records filtered to show only the records for that specific whitelist.

Network - IP Blacklists & Whitelists

IP blacklists and whitelists are used with **device flow correlation** (DFC) to define custom IP address detections. After you have created your lists you can then define in policy to use them in addition to the Cisco Intelligence Feed or on their own.

The lists can be defined using individual IP addresses, CIDR blocks, or IP address and port combinations. When you submit a list redundant addresses are combined on the back end.

For example if you add these entries to a list:

```
192.168.1.0/23
192.168.1.15
192.168.1.135
192.168.1.200
```

The list will be processed with a net result of:

```
192.168.1.0/23
```

However if you also include ports the result will be different:

```
192.168.1.0/23
192.168.1.15:80
192.168.1.135
192.168.1.200
```

The list will be processed with a net result of:

```
192.168.1.0/23
192.168.1.15:80
```

To black list or white list a port regardless of IP address, you can add two entries to the appropriate list where XX is the port number you want to block:

```
0.0.0.1/1:XX
128.0.0.1/1:XX
```

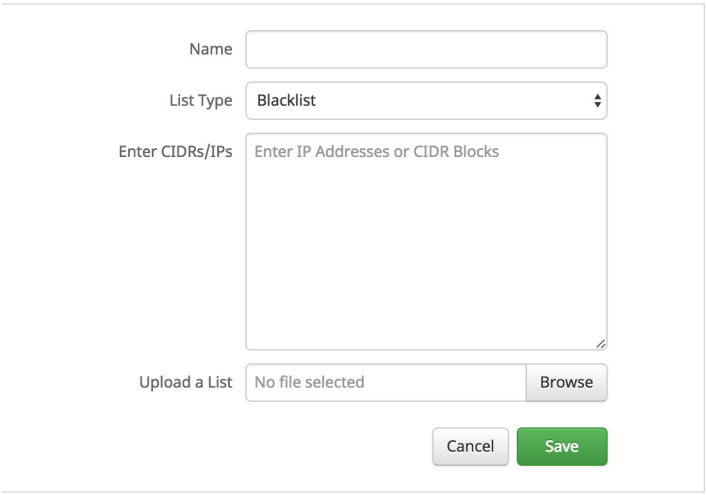
IMPORTANT! Uploaded IP lists can contain up to 100,000 lines or be a maximum of 2 MB in size. Only IPv4 addresses are currently supported.

Click the **View All Changes** link to see the Audit Log with all records filtered to show only IP blacklist and whitelist entries. Click **View Changes** next to a single IP list to view the Audit Log with all records filtered to show only the records for that specific list.

IP Blacklists

An **IP blacklist** allows you to specify IP addresses you want to detect any time one of your computers connects to them. You can choose to add a single IP address, an entire CIDR block, or specify an IP address and port number. When a computer makes a connection to an IP address in your list the action taken depends on what you have specified in the Network > Device Flow Correlation (DFC) section of your policy.

To create an IP blacklist go to **Outbreak Control > IP Blacklists & Whitelists** and click **Create IP List**. Give the list a name and select **Blacklist** from the **List Type** pull down. You can then either enter IP addresses, CIDR blocks, or IP address and port combinations in the field provided or upload a text file containing the addresses you want blocked. Once you have entered the addresses or uploaded your list, click **Create IP List** to save the list.

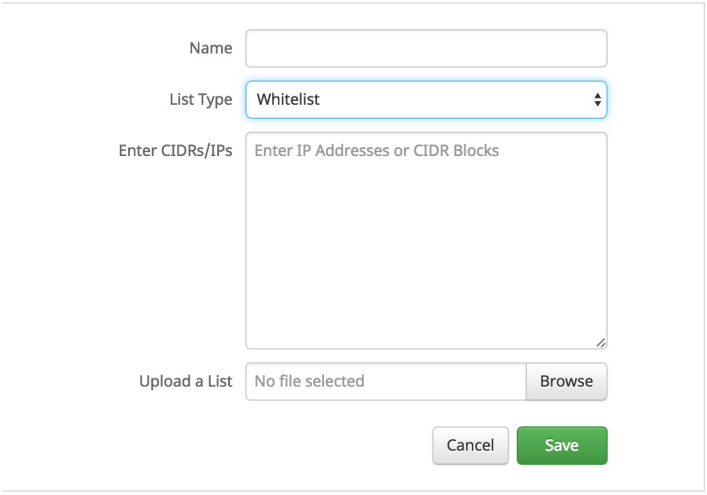


IP Whitelists

An **IP whitelist** allows you to specify IP addresses you never want to detect. Entries in your IP whitelist will override your IP blacklist as well as the Cisco Intelligence Feed. You can choose to add a single IP address, an entire CIDR block, or specify an IP address and port number.

To create an IP whitelist go to **Outbreak Control > IP Blacklists & Whitelists** and click **Create IP List**. Give the list a name and select **Whitelist** from the **List Type** pull down. You can then either enter IP addresses, CIDR blocks, or IP address and port combinations in the

field provided or upload a text file containing the addresses you want blocked. Once you have entered the addresses or uploaded your list, click **Create IP List** to save the list.



Editing IP Blacklists and Whitelists

To edit an IP list, navigate to **Outbreak Control > IP Black/White Lists**.

1. Locate the list you want to edit and click the **Download** link. This will download the list to your computer as a text file.
2. Open the text file and make any edits to the list, then save it.
3. In the AMP for Endpoints Console create a new IP blacklist or whitelist.
4. Upload your edited text file by clicking **Choose File**.
5. Click **Create IP List** to save your new list.

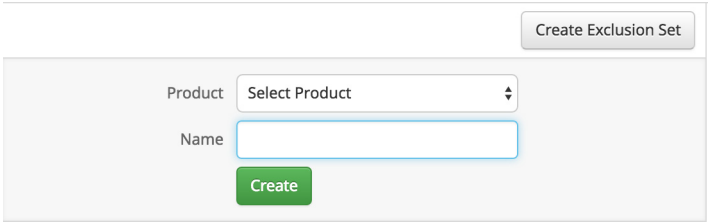
CHAPTER 4
EXCLUSIONS

An exclusion set is a list of directories, file extensions, or threat names that you do not want the AMP for Endpoints Connector to scan or convict. **Exclusions** can be used to resolve conflicts with other security products or mitigate performance issues by excluding directories containing large files that are frequently written to, such as databases. Use Application Control - Whitelisting to stop the AMP for Endpoints Connector from quarantining a single file (for example, a false positive detection). If you are running an antivirus product on computers with the AMP for Endpoints Connector, you will want to exclude the location where that product is installed.

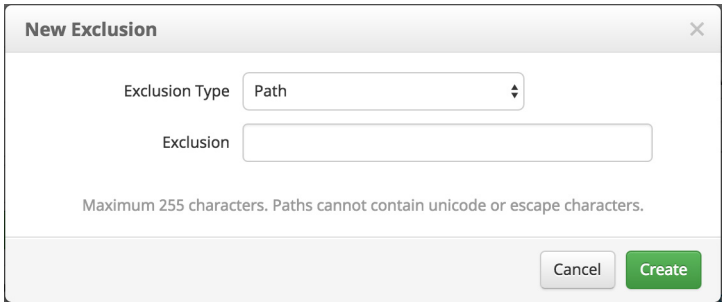
WARNING! Any files located in a directory that has been added to an exclusion list will not be subjected to application blocking, simple custom detections, or advanced custom detection lists.

Creating and Managing Exclusions

To create a custom exclusion set, go to **Management > Exclusions**. Click **Create Exclusion Set**, select whether the exclusions will be for AMP for Endpoints Windows, AMP for Endpoints Mac, or AMP for Endpoints Linux Connectors, give it a name, and click **Create**.



After you save the exclusion set, click **Edit** and you will see an **Add Exclusion** link. Clicking the **Add Exclusion** link will bring up a dialog box.



You can add a path, threat name, file extension, process, or use wild cards for file names, extensions, or paths, and then click **Create**. If you accidentally create an exclusion you do not want, you can click on the **Edit** button to expand the exclusion set, then select the specific exclusion and click **Delete**. Click **View All Changes** to see a filtered list of the Audit Log showing all exclusion set changes or click **View Changes** on a specific exclusion set to see changes made to just that particular set.

IMPORTANT! You cannot use wild cards or variables such as %windir% with CSIDLs.

If you add an exclusion by path on Windows, it is strongly suggested you use the CSIDL (http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx). These are variables on Windows computers in case the path is not the same on every system.

IMPORTANT! The CSIDLs are case sensitive.

Path exclusions are the most frequently used, as application conflicts usually involve excluding a directory. You can create a path exclusion using an absolute path or the CSIDL. For example, if you wanted to exclude an antivirus application in the Program Files directory, you could enter the exclusion path as:

```
C:\Program Files\MyAntivirusAppDirectory
```

IMPORTANT! You do not need to escape “space” characters in a path. For some non-English languages, different characters may represent path separators. The Connectors will only recognize '\' characters as valid path separators for exclusions to take effect.

However, if some computers in your organization have the Program Files directory on a different drive or path, you can use a CSIDL instead. So, the above exclusion path would instead be:

```
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
```

IMPORTANT! Path exclusions will prevent the AMP for Endpoints Connector from scanning all files and subdirectories in the directory specified.

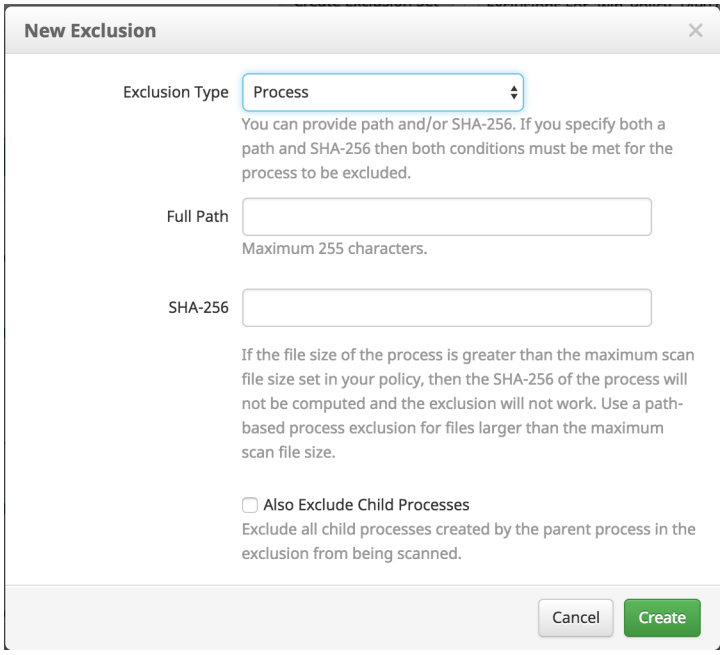
Wildcard exclusions are the same as path or extension exclusions except that you can use an asterisk character as a wild card. For example, if you wanted to exclude your virtual machines on a Mac from being scanned you might enter this path exclusion:

```
/Users/johndoe/Documents/Virtual Machines/
```

However, this exclusion will only work for one user, so instead replace the username in the path with an asterisk and create a wild card exclusion instead to exclude this directory for all users:

```
/Users/*/Documents/Virtual Machines/
```

Process exclusions allow you to exclude running processes from being scanned by the Connector and are only available in the AMP for Endpoints Windows Connector version 5.1.1 and higher.



You can exclude processes by specifying the full path to the process executable, the SHA-256 value of the process executable, or both the path and the SHA-256. You can enter either a direct path or use a CSIDL value. If you specify both the path and the SHA-256 for a process exclusion, then both conditions must be met for the process to be excluded.

IMPORTANT! If the file size of the process is greater than the maximum scan file size set in your policy, then the SHA-256 of the process will not be computed and the exclusion will not work. Use a path-based process exclusion for files larger than the maximum scan file size.

Child processes created by an excluded process are not excluded by default. For example, if you created a process exclusion for MS Word, by default any additional processes created by Word would still be scanned and appear in the Device Trajectory. This could be useful if you don't want to see every time MS Word runs in the Trajectory, but you want to see if a malicious Word document launches another application like a command shell. Select **Also Exclude**

Child Processes if you do not want any child processes to be scanned or appear in Device Trajectory.

File Extension exclusions allow you to exclude all files with a certain extension. For example, you might want to exclude all Microsoft Access database files by creating the following exclusion:

```
MDB
```

Threat exclusions let you exclude a particular threat name from triggering events. You should only ever use a Threat exclusion if you are certain that the events are the result of a false-positive detection. In that case, use the exact threat name from the event as your Threat exclusion. Be aware that if you use this type of exclusion even a true-positive detection of the threat name will not appear in your events.

Antivirus Compatibility Using Exclusions

To prevent conflicts between the AMP for Endpoints Connector and antivirus or other security software, you must create exclusions so that the AMP for Endpoints Connector doesn't scan your antivirus directory and your antivirus doesn't scan the AMP for Endpoints Connector directory. This can create problems if antivirus signatures contain strings that the AMP for Endpoints Connector sees as malicious or issues with quarantined files.

Creating Antivirus Exclusions in the AMP for Endpoints Connector

1. The first step is to create an exclusion by navigating to **Management > Exclusions** in the AMP for Endpoints Console.
2. Click on **Create Exclusion Set** to create a new list of exclusions. Enter a name for the list and click **Create**.
3. Next click **Add Exclusion** to add an exclusion to your list.
4. You will then be prompted to enter a path for the exclusion. Enter the CSIDL of the security products you have installed on your endpoints then click **Create**.

Repeat this procedure for each path associated with your security applications. Common CSIDLs for security products that should be excluded are as follows.

Kaspersky

- CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data

McAfee VirusScan Enterprise

- CSIDL_PROGRAM_FILES\McAfee
- CSIDL_PROGRAM_FILESX86\McAfee
- CSIDL_PROGRAM_FILES\Common Files\McAfee
- CSIDL_COMMON_APPDATA\McAfee
- CSIDL_PROGRAM_FILES\VSE
- CSIDL_COMMON_APPDATA\VSE
- CSIDL_PROGRAM_FILES\Common Files\VSE

Microsoft ForeFront

- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILESX86\Microsoft Forefont

Microsoft Security Client

- CSIDL_PROGRAM_FILES\Microsoft Security Client
- CSIDL_PROGRAM_FILESX86\Microsoft Security Client

Sophos

- CSIDL_PROGRAM_FILES\Sophos
- CSIDL_PROGRAM_FILESX86\Sophos
- CSIDL_COMMON_APPDATA\Sophos\Sophos Anti-Virus\

Splunk

- CSIDL_PROGRAM_FILES\Splunk

Symantec Endpoint Protection

- CSIDL_COMMON_APPDATA\Symantec
- CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection

Once you have added all the necessary exclusions for your endpoints, you will need to add the exclusion set to a policy.

Creating Exclusions in Antivirus Software

In addition to creating exclusions for antivirus products in the AMP for Endpoints Connector, you must also create exclusions for the AMP for Endpoints Connector in antivirus products running on your endpoints. The following are the steps for doing this in common antivirus products.

Creating Exclusions in McAfee ePolicy Orchestrator 4.6

1. Log in to ePolicy Orchestrator.
2. Select **Policy** >**Policy Catalog** from the menu.
3. Select the appropriate version of VirusScan Enterprise from the **Product** pull-down.
4. Edit your On-Access High-Risk Processes Policies.
5. Select the **Exclusions** tab and click the **Add** button.

6. In the **By Pattern** field, enter the path to your AMP for Endpoints Connector install (C:\Program Files\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) and check the **Also exclude subfolders** box.

   IMPORTANT! You should exclude the AMP for Endpoints Connector using the Sourcefire directory as other files and sub-folders

7. Click **OK**.
8. Click **Save**.
9. Edit your On-Access Low-Risk Processes Policies.
10. Repeat steps 5 through 8 for this policy.

Creating Exclusions in McAfee VirusScan Enterprise 8.8

1. Open the VirusScan Console.
2. Select **On-Access Scanner Properties** from the **Task** menu.
3. Select **All Processes** from the left pane.
4. Select the **Exclusions** tab.
5. Click the **Exclusions** button.
6. On the **Set Exclusions** dialog click the **Add** button.
7. Click the **Browse** button and select your AMP for Endpoints Connector install directory (C:\Program Files\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) and check the **Also exclude subfolders** box.
8. Click **OK**.
9. Click **OK** on the **Set Exclusions** dialog.
10. Click **OK** on the **On-Access Scanner Properties** dialog.

Creating Exclusions in a Managed Symantec Enterprise Protection 12.1 Install

1. Log into Symantec Enterprise Protection Manager.
2. Click **Policies** in the left pane.
3. Select the **Exceptions** entry under the **Policies** list.
4. You can either add a new exceptions policy or edit an existing one.
5. Once you have opened the policy, click **Exceptions**.
6. Click the **Add** button, select **Windows Exceptions** from the list and choose **Folder** from the sub-menu.
7. In the **Add Security Risk Folder Exception** dialog, choose [PROGRAM_FILES] from the **Prefix variable** drop-down menu and enter Cisco for Connector versions 5.1.1 and higher or Sourcefire for previous versions in the Folder field. Ensure that **Include subfolders** is checked.

8. Under **Specify the type of scan that excludes this folder** menu, select **All**.
9. Click **OK**.
10. Make sure that this exception is used by all computers in your organization with the AMP for Endpoints Connector installed.

Creating Exclusions in an Unmanaged Symantec Enterprise Protection 12.1 Install

1. Open Symantec Enterprise Protection and click on **Change Settings** in the left pane.
2. Click **Configure Settings** next to the **Exceptions** entry.
3. Click the **Add** button on the **Exceptions** dialog.
4. Select **Folders** from the **Security Risk Exception** sub-menu.
5. Select your AMP for Endpoints Connector installation directory (C:\Program Files\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) from the dialog and click **OK**.
6. Click the **Add** button on the **Exceptions** dialog.
7. Select **Folder** from the **SONAR Exception** sub-menu.
8. Select your AMP for Endpoints Connector installation directory (C:\Program Files\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) from the dialog and click **OK**.
9. Click the **Close** button.

Creating Exclusions for the AMP for Endpoints Connector in Microsoft Security Essentials

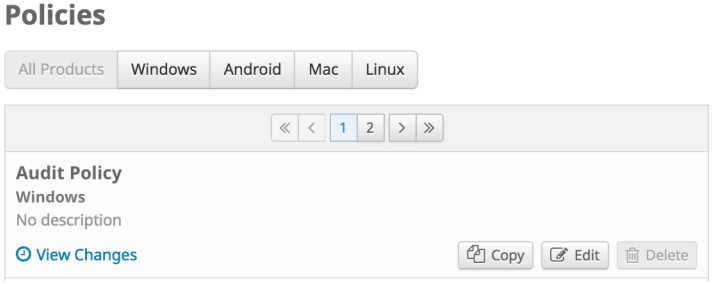
1. Open **Microsoft Security Essentials** and click on the **Settings** tab.
2. Select **Excluded files and locations** in the left pane.
3. Click the **Browse** button and navigate to your AMP for Endpoints Connector installation directory (C:\Program Files\Cisco for versions 5.1.1 and higher or C:\Program Files\Sourcefire for previous versions by default) and click **OK**.
4. Click the **Add** button then click **Save** changes.
5. Select **Excluded processes** in the left pane.
6. Click the **Browse** button and navigate to the sfc.exe file (C:\Program Files\Cisco\AMP\x.x.x.x\sfc.exe for versions 5.1.1 and higher or C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe for previous versions by default where x.x.x is the AMP for Endpoints Connector version number) and click **OK**.
7. Click the **Add** button then click **Save** changes.

IMPORTANT! Because the process exclusions in Microsoft Security Essentials require a specific path to the sfc.exe file you will need to update this exclusion whenever you upgrade to a new version of the AMP for Endpoints Connector.

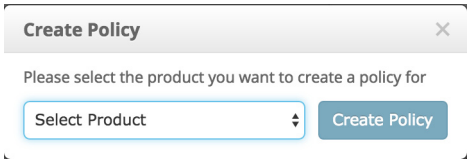
CHAPTER 5
POLICIES

IMPORTANT! You can preview the upcoming redesigned Policies UI by clicking the "Try the new Policies UI" link in the header of the Policies page.

Outbreak Control and Exclusions lists are combined with other settings into a policy. The policy affects the behavior and certain settings of the Connector. A policy is applied to a computer via Groups.



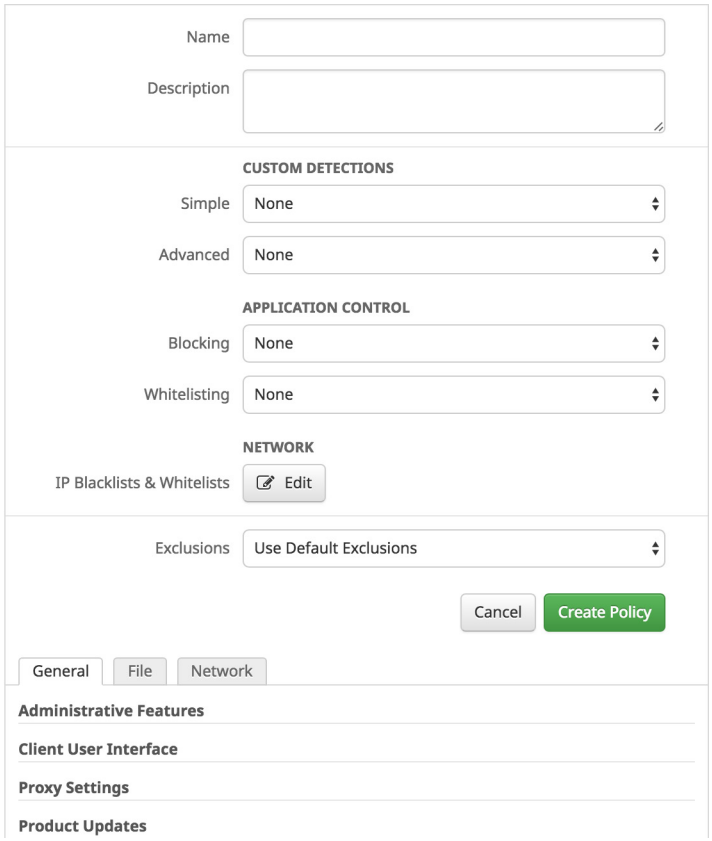
Click **Create Policy** to create a new policy or **Copy** if you want to create a new policy based on an existing one. Next, choose whether you want to create a policy for AMP for Endpoints Windows, AMP for Endpoints Android, or AMP for Endpoints Mac. **View Changes** will take you to a filtered view of the Audit Log showing all the changes for that specific policy. You can also use **View All Changes** at the top of the page to show changes to all policies.



This will take you to the **New Policy** page. The configuration is discussed below.

Policy Contents

There are numerous settings that can be set in the policy. This section will detail each one. AMP for Endpoints Windows and AMP for Endpoints Mac both share some basic policy settings.

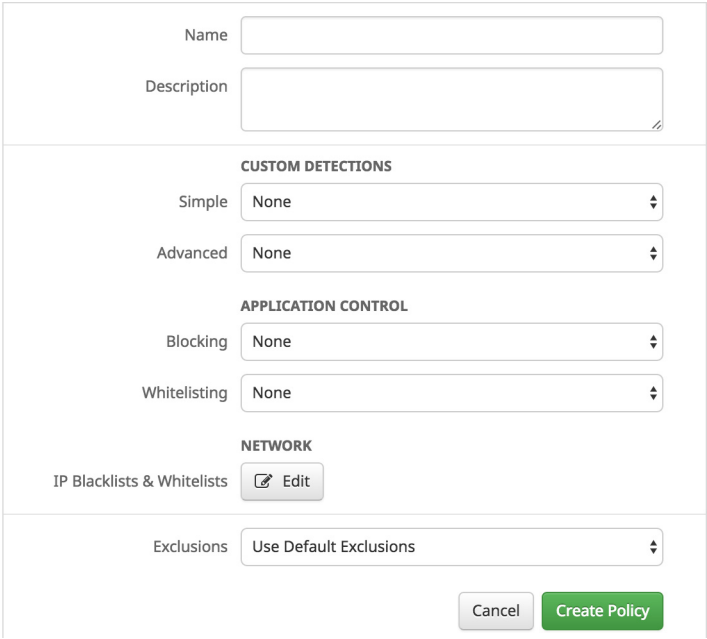


IMPORTANT! If Cisco Defense Center is integrated with AMP for Endpoints, the Network policy contains some of these settings. For more information on Defense Center integration with AMP for Endpoints, see your Defense Center documentation.

Name, Lists, and Description

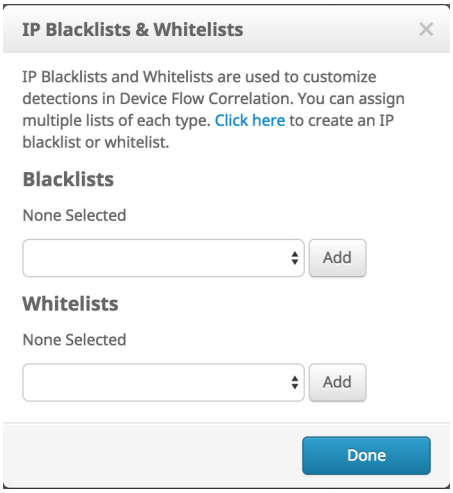
The **Name** box allows you to create a name that you can use to recognize the policy. Select the lists you want to assign to the policy. See Custom Detections - Simple, Custom Detections - Advanced, Application Control - Blocking, Application Control - Whitelisting, Network - IP

Blacklists & Whitelists, and Exclusions for details on creating these lists. Not all Connectors support all list types. The description can be used to give more description about the policy.



IMPORTANT! IP blacklists and IP whitelists will only work if you enable DFC under Device Flow Correlation in the Network tab of your policy.

When you click IP blacklists and IP whitelists **Edit** button a dialog appears to select your lists.



Select the list you want to add from the drop-down menu and click **Add**. You can add multiple IP lists to a single policy; however, IP whitelist entries will override IP blacklist entries.

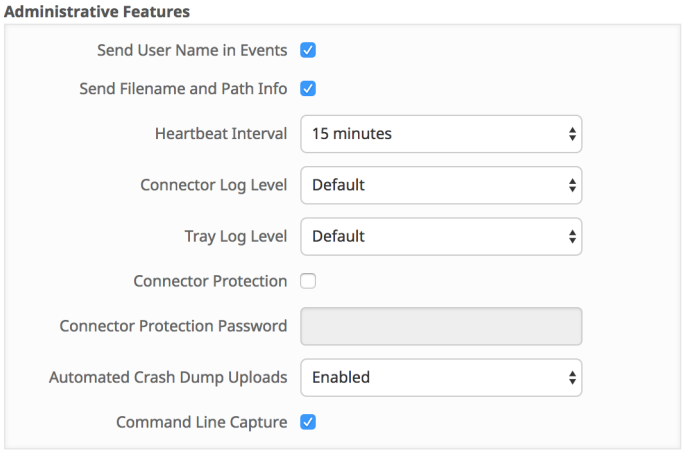
AMP for Endpoints Windows Connector

This section describes the policy options that are available for AMP for Endpoints Windows Connectors. The options are divided into three tabs: **General**, **File**, and **Network**.

General Tab

The **General** tab contains overall settings for your AMP for Endpoints Connectors, such as proxy settings, update schedules, and general administrative settings.

General > Administrative Features



Send User Name in Events will send the actual user name for which the process is executed, copied, or moved as if known. This is useful for tracking down who is seeing malware. If this is not enabled, you will see a "u" for malware executed, copied, or moved as a user and an "a" for something that has been executed copied or moved as an administrator.

Send Filename and Path Info will send the filename and path information to AMP for Endpoints so that they are visible in the Events Tab, Device Trajectory, and File Trajectory. Unchecking this setting will stop this information from being sent.

The **Heartbeat Interval** is the frequency with which the Connector calls home to see if there are any files to restore via Retrospective or by the administrator, any policies to pick up, or any tasks to perform such as product updates or scans.

Connector Log Level and **Tray Log Level** allow you to choose between default and debug (verbose) logging levels. The default level should be set unless debug is requested by support during troubleshooting.

WARNING! When **Connector Log Level** is set to **Debug,** it can cause log files to consume an additional 550MB of drive space.

Connector Protection allows you to require a password to uninstall the AMP for Endpoints Connector or stop its service. This setting only applies to version 3.1.0 and higher of the AMP for Endpoints Connector.

Connector Protection Password is the password you supply to **Connector Protection** to stop the AMP for Endpoints Connector service or uninstall it.

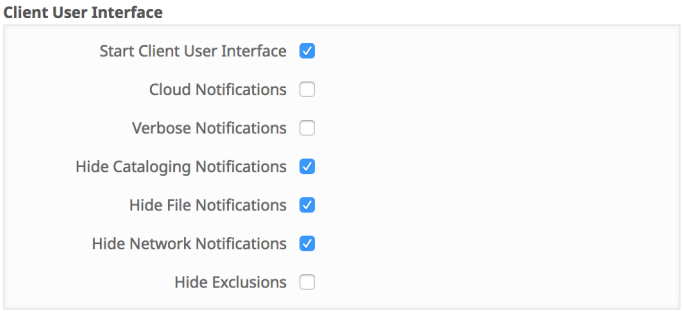
IMPORTANT! If you enable **Connector Protection** on a policy that includes previously deployed Connectors, you must reboot the computer or stop and restart the Connector service for this setting to take effect.

Automated Crash Dump Uploads allows you to choose whether to automatically upload AMP for Endpoints Connector crash dump files to Cisco for analysis.

Command Line Capture (AMP for Endpoints Windows 5.0 and higher) allows the Connector to capture command line arguments (including usernames, filenames, passwords, etc.) used during file execution and send the information to AMP for Endpoints. This information will be displayed in Device Trajectory for administrators as long as they have Two-Step Verification enabled.

If **Command Line Capture** is enabled and **Connector Log Level** is set to **Debug**, you can use **Command Line Logging** to log captured command line arguments to the local Connector log file on the endpoint.

General > Client User Interface



Start Client User Interface allows you to specify whether or not to completely hide the Connector user interface. Unchecking this option will let the Connector run as a service but the user interface components will not run.

IMPORTANT! If you change this setting, your Connectors will have to be restarted before it takes effect.

Cloud Notifications are balloon pop-ups that come from the Windows system tray when the AMP for Endpoints Connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud.

Verbose Notifications are boxes that pop-up from the Windows system tray that tell the user when they are copying a trusted file. This should be turned off unless troubleshooting.

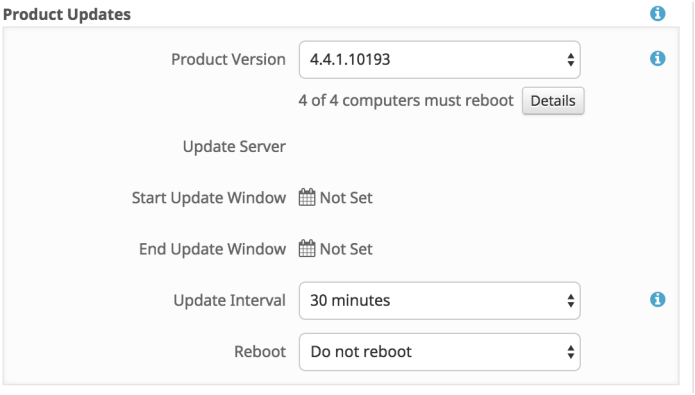
Hide File Notifications suppresses notifications from being displayed to the user when a malicious file is convicted or quarantined by the Connector.

Hide Cataloging Notifications suppresses notifications to the user about cataloging before full endpoint IOC scans.

Hide Network Notifications suppresses notifications from being displayed to the user when a malicious network connection is detected or blocked by the Connector.

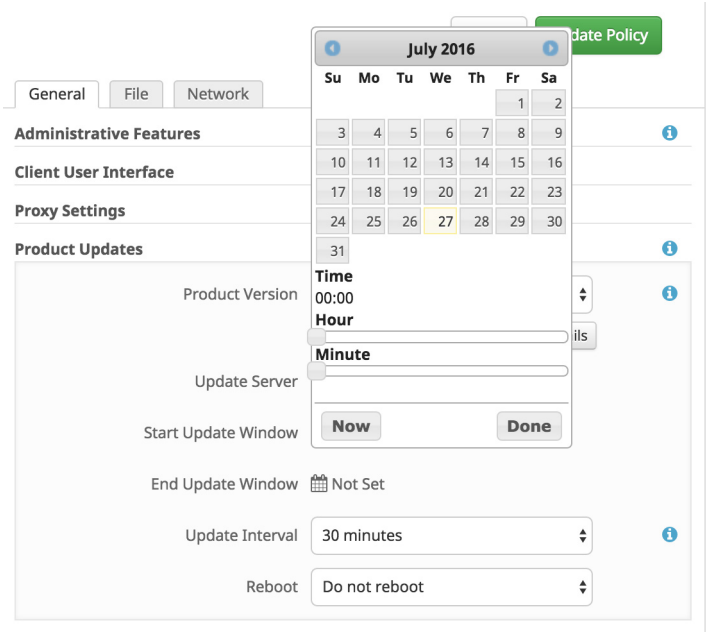
Hide Exclusions will suppress the display of configured exclusions from the Connector user interface. (Available on AMP for Endpoints Windows Connector versions 5.1.3 and higher)

General > Product Updates



When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** showing which version you are going to and it will populate the **Update Server** so you can see where the files will be pulled from. There will also be information to show how many Connectors in groups that use the policy will require a reboot after updating. You can then configure the **Start Update Window** and **End Update Window**. The **Update Interval** allows you to specify how long

your Connectors will wait between checks for new product updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic.



Start Update Window allows you to choose a date and time at which the updates can start occurring.

End Update Window allows you to choose a date and time at which the updates will stop occurring.

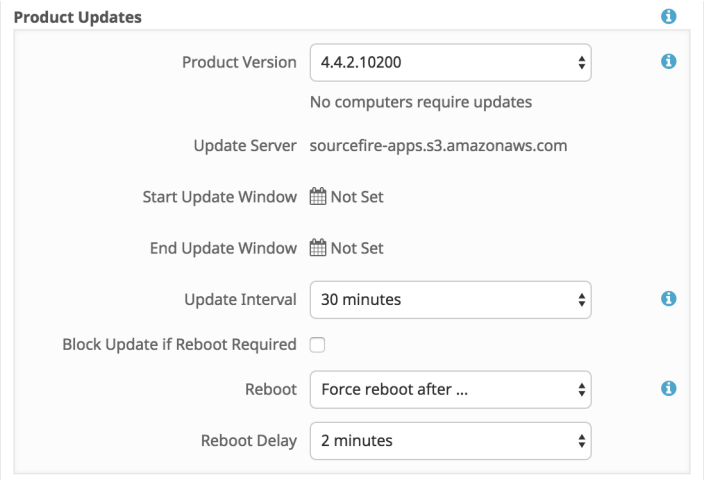
Between the **Start Update Window** and the **End Update Window**, if a Connector calls home to pick up a policy, it will pick up the product update. Because the Connector calls home at an interval dependent on the Heartbeat Interval, you will want to plan your Update Window accordingly; that is, make sure the interval specified in the Update Window is larger than the Heartbeat Interval.

Reboot gives you the options **Do not reboot**, **Ask for reboot** from the user, or **Force reboot after 2 minutes**.

IMPORTANT! The computer will need to be rebooted for the updated AMP for Endpoints Connector to work properly.

On Windows 8 and higher, if **Fast Startup** mode or **Hibernation** is enabled, you should reboot the computer after the update is complete rather than using the Windows shutdown option. This will ensure that the final steps to update the Connector drivers complete properly.

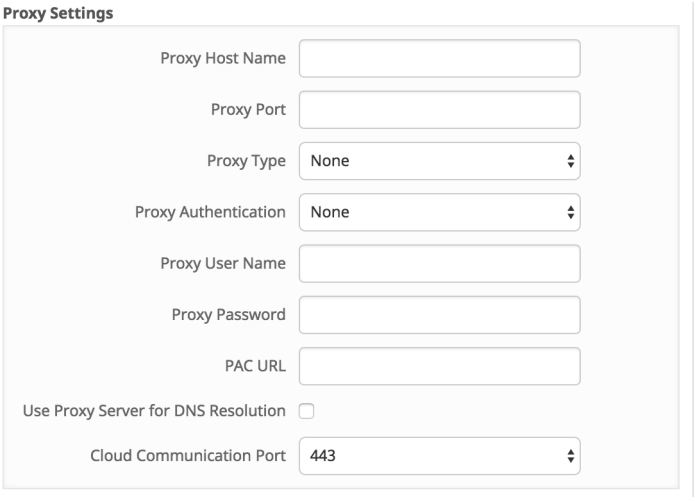
If you are updating to version 4.3 or later of the AMP for Endpoints Windows Connector you will be given different reboot options. As of version 4.3 some updates may not require a reboot to take effect.



Check **Block Update if Reboot Required** to prevent the Connector from updating if the update requires a reboot. This is useful for servers or high-availability computers for which you would prefer to perform the update manually if a reboot is required. Optionally, you can set a new update window for a period where some downtime is acceptable.

The **Reboot** behavior still includes **Do not reboot** and **Ask for reboot**, but you can also select **Force reboot after...** and specify the **Reboot Delay**. This value can be set to **2 minutes**, **10 minutes**, or **30 minutes**.

General > Proxy Settings



Proxy Host Name is the name or IP of the proxy server.

Proxy Port is the port the proxy server runs on.

Proxy Type is the type of proxy you are connecting to. The Connector will support **http_proxy**, **socks4**, **socks4a**, **socks5**, and **socks5_hostname**.

Proxy Authentication is the type of authentication used by your proxy server. **Basic** and **NTLM** authentication are supported.

Proxy User Name is used for authenticated proxies. This is the user name you use to connect.

IMPORTANT! If NTLM is selected as the proxy authentication type, this field must be in domain\username format.

Proxy Password is used for authenticated proxies. This is the password you use with the Proxy Username.

PAC URL allows you to specify a location for the Connector to retrieve the proxy auto-config (PAC) file.

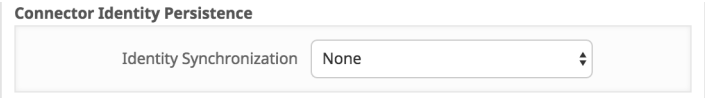
IMPORTANT! The URL must specify HTTP or HTTPS when defined through policy and only ECMAScript-based PAC files with a .pac extension are supported. If the PAC file is hosted on a Web server, the proper MIME type of application/x-javascript-config must be specified.

Use Proxy Server for DNS Resolution lets you specify whether all Connector DNS queries should be performed on the proxy server.

Cloud Communication Port allows you to select whether your Connectors perform cloud lookups on TCP **32137** or **443**.

General > Connector Identity Persistence

IMPORTANT! This policy setting is only available when enabled by Amp for Endpoints Support. If you feel you need this feature, contact Support to enable it.



Identity Synchronization allows you to maintain a consistent event log in virtual environments or when computers are re-imaged. You can bind a Connector to a MAC address or host name so that a new event log is not created every time a new virtual session is started or a computer is re-imaged. You can choose to apply this setting with granularity across different policies, or across your entire organization, as follows.

- **None**: Connector logs are not synchronized with new Connector installs under any circumstance.
- **By MAC Address across Business**: New Connectors look for the most recent Connector that has the same MAC address to synchronize with across all policies in the business that have Identity Synchronization set to a value other than None.
- **By MAC Address across Policy**: New Connectors look for the most recent Connector that has the same MAC address to synchronize with within the same policy.

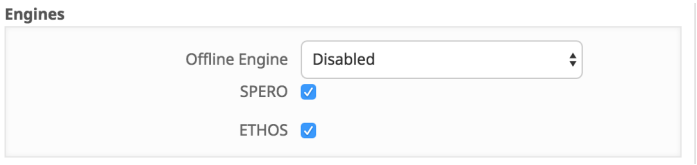
- **By Hostname across Business**: New Connectors look for the most recent Connector that has the same hostname to synchronize with across all policies in the business that have Identity Synchronization set to a value other than None.
- **By Hostname across Policy**: New Connectors look for the most recent Connector that has the same hostname to synchronize with within the same policy.

IMPORTANT! In some cases a cloned virtual machine may be placed in the **Default Group** rather than the group from which it was cloned. If this occurs, move the virtual machine into the correct group in the AMP for Endpoints Console.

File Tab

The **File** tab contains settings for the file scanning engine behaviors of your AMP for Endpoints Connectors, such as which engines to use, setting up scheduled scans, and cache settings.

File > Engines

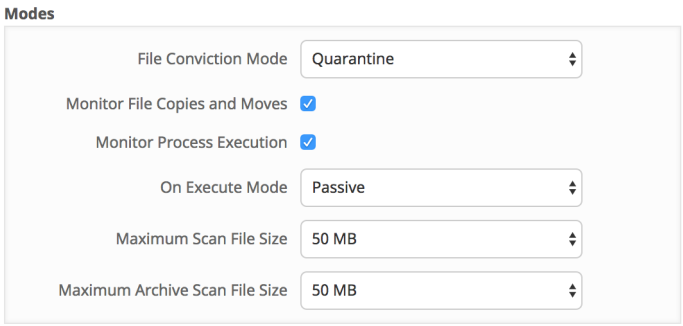


Offline Engine can be set to **Disabled** or **TETRA**. TETRA is a full antivirus replacement and should never be enabled if another antivirus engine is installed. TETRA can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment. When this is set to TETRA, another menu will appear to allow you to configure TETRA.

SPERO is the Cisco machine-based learning system. We use hundreds of features of a file, which we call a SPERO fingerprint. This is sent to the cloud and SPERO trees determine whether a file is malicious.

ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.

File > Modes



File Conviction Mode allows you to specify the action the Connector takes when a malicious file is convicted. Setting this to **Audit** will stop the AMP for Endpoints Connector from quarantining any files. This setting only applies to version 3.1.0 and higher of the AMP for Endpoints Connector.

WARNING! When **File Conviction Mode** is set to **Audit,** any malicious files on your endpoints will remain accessible and be allowed to execute. Application blocking lists will also not be enforced. You should only use this setting for testing purposes with proprietary software.

Monitor File Copies and Moves is the ability for the AMP for Endpoints Connector to give real-time protection to files that are copied or moved.

Monitor Process Execution is the ability for the AMP for Endpoints Connector to give real-time protection to files that are executed.

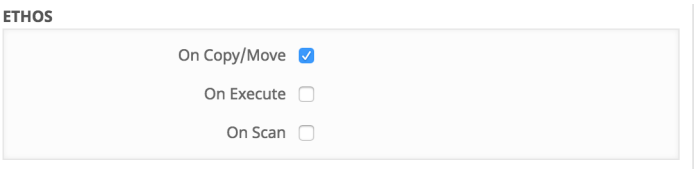
On Execute Mode can run in two different modes: **Active** or **Passive**. In Active mode, the file is blocked from being executed until a determination of whether or not a file is malicious or a timeout is reached. In Passive mode, the file is allowed to be executed and in parallel the file is looked up to determine whether or not it is malicious.

WARNING! Although Active mode gives you better protection, it can cause performance issues. If the endpoint already has an antivirus product installed it is best to leave this set to Passive.

Maximum Scan File Size limits the size of files that are scanned by the AMP for Endpoints Connector. Any file larger than the threshold set will not be scanned.

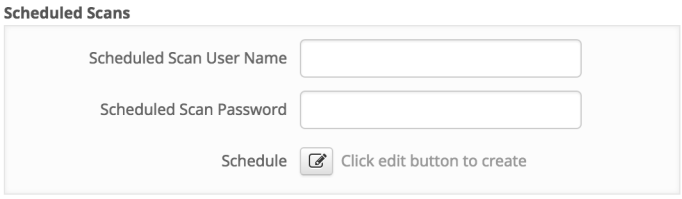
Maximum Archive Scan File Size limits the size of archive files that are scanned by the AMP for Endpoints Connector. Any archive file larger than the threshold set will not be scanned.

File > ETHOS



ETHOS is an engine for grouping files together, but can be resource intensive. That is why it is only turned on by default for **On Copy/Move**, but it can be turned on for **On Execute** and **On Scan**. However, turning it on for execute and scan will slow down these processes. When ETHOS does On Copy/Move scanning, the Connector allows the copy or move to complete and then queues another thread to calculate the ETHOS for a file to try and reduce the slow down.

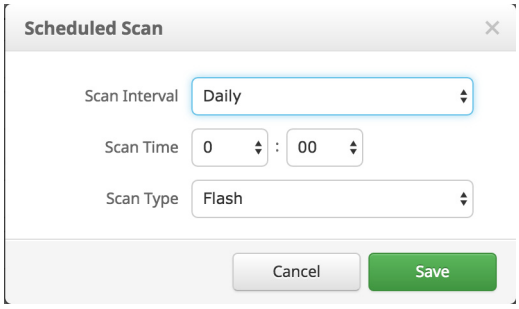
File > Scheduled Scans



Scheduled scans are not necessary for the operation of the AMP for Endpoints Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Retrospective. This allows companies to reduce their energy footprint by eliminating the need for scheduled scans. However, some companies may require scheduled scans due to policy so this can be enabled via policy when necessary.

Scheduled Scan Username requires the username on the local computer or domain the scan performs as. **Scheduled Scan Password** requires the password used for the Scheduled Scan Username account.

When you click **Schedule**, an overlay will come up to allow you to choose the scan interval, scan time, and scan type.



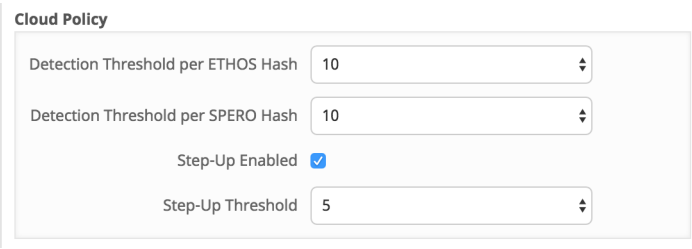
Scan Interval allows you to set how often the should run. The options are **Weekly** or **Monthly**.

Scan Time allows you to set the time of day you want the scan to commence.

Scan Type allows you to set the type of scan. A **Flash** scan will scan the processes running and the files and registry entries used by those processes. A **Full** scan will scan the processes

running, the registry entries, and all the files on disk. This scan is very resource-intensive and should not be performed on a regular basis. If TETRA is enabled it will perform a **Rootkit** scan as well. A **Custom** scan will scan a particular path that you give it.

File > Cloud Policy



ETHOS and SPERO are both considered generic engines. Because of this, the user has the ability to control how false positive-prone an ETHOS or SPERO hash is.

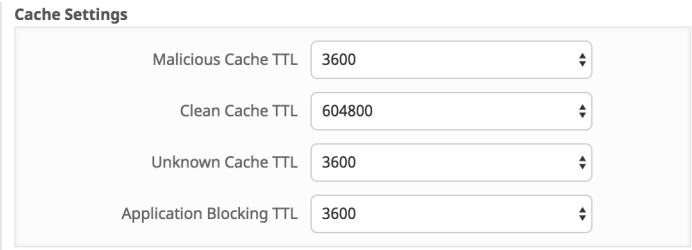
Detection Threshold per ETHOS Hash means that a single ETHOS hash can convict a single SHA of unknown disposition a maximum number of times. The default is 10, meaning that ETHOS will not convict any SHA-256 that is seen 10 times in 24 hours by the entire community. If you encounter a situation where the detection threshold has been reached but feel that the detection is not a false-positive and want to keep convicting the particular SHA, you should add it to a Custom Detections - Simple or Custom Detections - Advanced list.

Detection Threshold per SPERO Tree means that a single SPERO tree can convict a single SHA of unknown disposition a maximum number of times. The default is 10, meaning that SPERO will not convict any SHA-256 that is seen 10 times in 24 hours by the entire community. If you encounter a situation where the detection threshold has been reached but feel that the detection is not a false-positive and want to keep convicting the particular SHA, you should add it to a Custom Detections - Simple or Custom Detections - Advanced list.

Step-Up Enabled is the ability to turn on additional SPERO trees if you are considered "massively infected". These SPERO trees are more false positive-prone, but do a better job of detecting malware. "Massively infected" is based on the step-up threshold.

The **Step-Up Threshold** is used to determine whether or not a Connector is "massively infected". The default is 5, meaning that if 5 SHA one-to-one detections are found in 30 seconds, you are considered "massively infected" and additional SPERO trees will be enabled for the next 30 seconds.

File > Cache Settings



SHA-256 values are cached to reduce cloud lookup traffic. The amount of time a value is cached depends on the disposition of the file the last time a cloud lookup was performed on its SHA-256. While a file is cached, the Connector will always consider its disposition to be what it was the last time a cloud lookup was performed. For example, if a SHA-256 is in an application blocking list and the TTL is 3600 seconds, that application will continue to be blocked from execution by the Connector for the next hour even if the administrator removes it from the application blocking list.

Malicious Cache TTL is the time in seconds for which a file with a malicious disposition will be cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

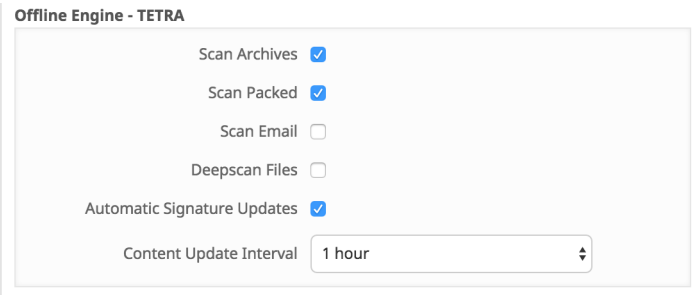
Clean Cache TTL is the time in seconds for which a file with a clean disposition will be cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 7 days.

Unknown Cache TTL is the time in seconds for which a file with an unknown disposition is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

Application Blocking TTL is the time in seconds for which a file that is in an Application Control - Blocking list is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

IMPORTANT! If you add a SHA-256 with a clean disposition that was previously seen by a Connector to an application blocking list, you must stop the Connector and delete the cache.db file from the installation directory on that computer for the application to be blocked from executing. Otherwise, you will have to wait until the TTL for the clean file expires and another cloud lookup is performed by the Connector before the application is blocked from executing.

File > Offline Engine - TETRA



TETRA performs offline scanning, rootkit scanning, and other things that a traditional antivirus product does. It is signature-based and will take up more disk space on the local computers. TETRA will check for updated signatures hourly and download them if new signatures are available. Its major drawback is compatibility with other antivirus products and it should never be enabled if another antivirus product is installed on the computer. This policy configuration option is only available when TETRA has been selected as the **Offline Engine** under **Engines**.

Scan Archives determines whether or not the Connector will open compressed files and scan their contents. The default limitation is not to look inside any compressed files over 50MB.

Scan Packed determines whether the Connector will open packed files and scan their contents.

Scan Email determines whether the Connector scans the contents of client email files. Supported email formats are Thunderbird 3.0.4, Outlook 2007, Outlook 2010, Windows Mail on x86, and Outlook Express.

Deepscan Files determines whether the Connector scans the contents of product install and CHM files.

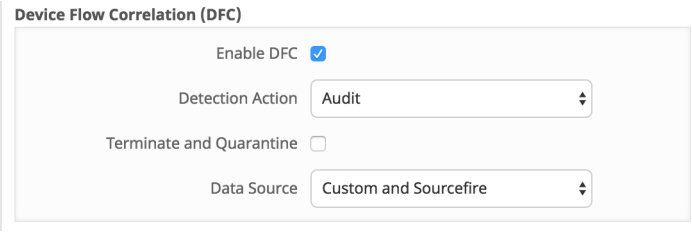
Automatic Signature Updates allows the Connector to automatically update its TETRA signatures. TETRA signature updates can consume significant bandwidth, so caution should be exercised before enabling automatic signature updates in a large environment.

Content Update Interval lets you specify how often your Connectors should check for new TETRA content such as signatures. Longer update intervals will help to reduce network traffic caused by TETRA updates while shorter update intervals can consume significant bandwidth and is not recommended for large deployments.

Network Tab

The **Network** tab contains settings to for the network flow capabilities of your AMP for Endpoints Connectors, such as device flow correlation settings.

Network > Device Flow Correlation (DFC)



Enable DFC will enable device flow correlation on your AMP for Endpoints Connector. This allows you to monitor network activity and determine which action the Connector should take when connections to malicious hosts are detected.

Detection Action allows you to select whether the Connector will block network connections to malicious hosts or simply log them.

Terminate and quarantine will allow the Connector to terminate the parent process of any connection to a malicious host if the process originated from a file with an unknown disposition.

WARNING! Before enabling this feature, make sure you have whitelisted any applications allowed in your environment, particularly any proprietary or custom software.

Data Source allows you to select the IP blacklists your Connectors use. If you select **Custom**, your Connectors will only use the IP blacklists you have added to the policy. Choose **Cisco** to

have your Connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by the Cisco VRT to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If the VRT continues to observe poor behavior related to an address it will be added back to the list. The **Custom and Cisco** option will allow you to use both the IP Blacklists you have added to the policy and the Cisco Intelligence Feed.

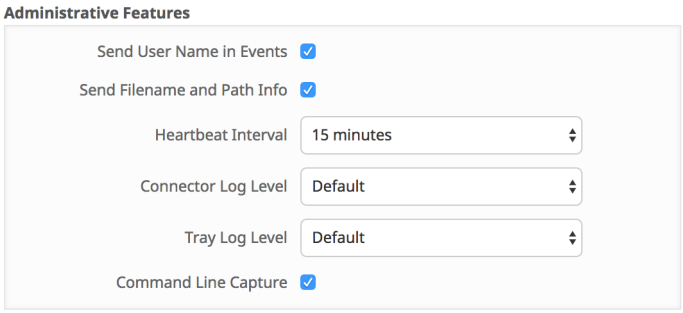
AMP for Endpoints Mac Connector

This section describes the policy options that are available for AMP for Endpoints Mac Connectors. The options are divided into three tabs: **General**, **File**, and **Network**.

General Tab

The **General** policy tab contains overall settings for your AMP for Endpoints Connectors such as proxy settings, update schedules, and general administrative settings.

General > Administrative Features



Send User Name in Events (available for AMP for Endpoints Mac Connector version 1.3.0 and later) will send the actual user name for which the process is executed, copied, or moved as if known. This is useful for tracking down who is seeing malware. If this is not enabled, you will see a “u” for malware executed, copied, or moved as a user and “a” for something executed copied or moved as an administrator.

Send Filename and Path Info sends the filename and path to the Cisco Cloud so that the information can be displayed in **Events** when viewed in the Console.

The **Heartbeat Interval** is the interval at which the Connector calls home to see if there are any files to restore via Retrospective or by the administrator, any policies to pick up, or any tasks to perform such as product updates or scans.

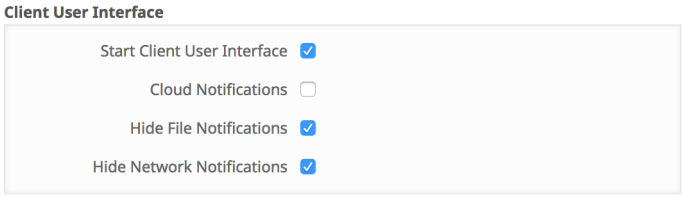
Connector Log Level and **Tray Log Level** allow you to choose between default and debug (verbose) logging levels. The default level should be set unless debug is requested by support during troubleshooting.

Command Line Capture (AMP for Endpoints Mac 1.3 and higher) allows the Connector to capture command line arguments (including usernames, filenames, passwords, etc.) used during file execution and send the information to AMP for Endpoints. This information will be

displayed in Device Trajectory for administrators as long as they have Two-Step Verification enabled.

If **Command Line Capture** is enabled and **Connector Log Level** is set to **Debug**, you can use **Command Line Logging** to log captured command line arguments to the local Connector log file on the endpoint.

General > Client User Interface



Start the Client User Interface allows you to specify whether or not to completely hide the Connector user interface. Unchecking this option will let the Connector run as a service but the user interface components will not run.

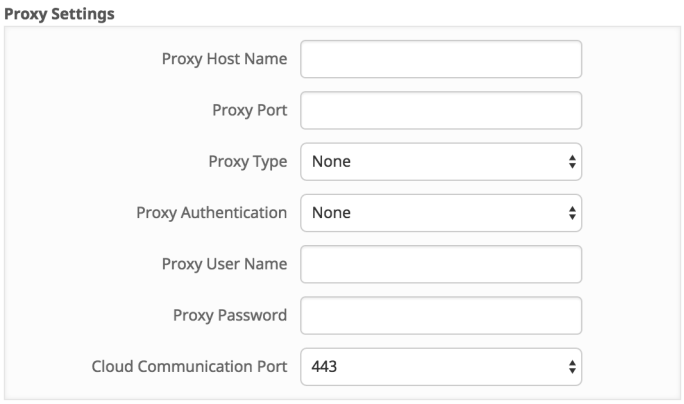
IMPORTANT! If you change this setting, your Connectors will have to be restarted before it takes effect.

Cloud Notifications are balloon pop-ups that come from the **Notification Center** when the AMP for Endpoints Connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud.

Hide File Notifications suppresses notifications from being displayed to the user when a malicious file is convicted or quarantined by the Connector.

Hide Network Notifications suppresses notifications from being displayed to the user when a malicious network connection is detected or blocked by the Connector.

General > Proxy Settings



Proxy Host Name is the name or IP of the proxy server.

Proxy Port is the port the proxy server runs on.

Proxy Type is the type of proxy you are connecting to. The Connector supports **http_proxy**, **socks4**, **socks4a**, **socks5**, and **socks5_hostname**.

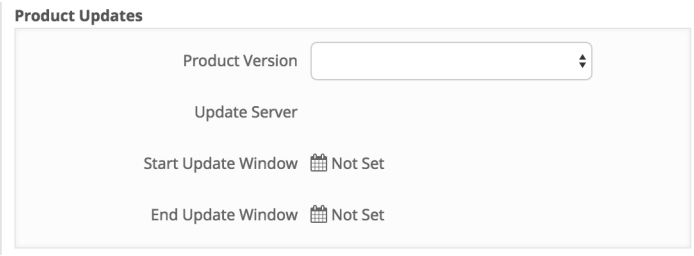
Proxy Authentication is the type of authentication used by your proxy server. **Basic** and **NTLM** authentication are supported.

Proxy User Name is used for authenticated proxies. This is the user name you use to connect.

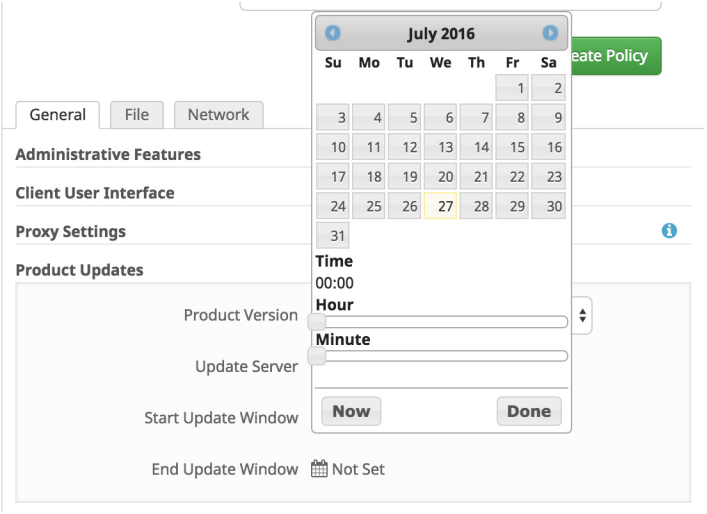
Proxy Password is used for authenticated proxies. This is the password you use with the **Proxy User Name**.

Cloud Communication Port allows you to select whether your Connectors perform cloud lookups on TCP **32137** or **443**.

General > Product Updates



When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** that shows which version you are going to and it will populate the **Update Server** so you can see where the files will be pulled from. You can then configure the **Start Update Window** and **End Update Window**.



Start Update Window allows you to choose a date and time at which the updates can start occurring.

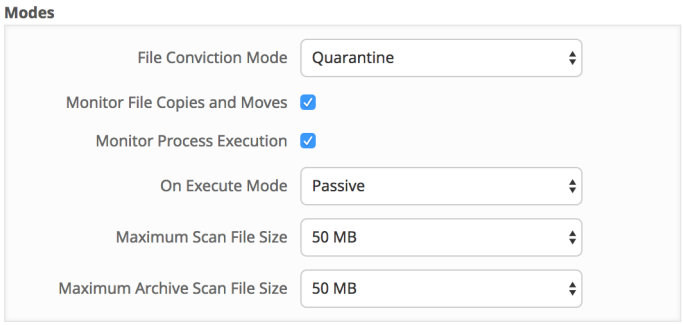
End Update Window allows you to choose a date and time at which the updates will stop occurring.

Between the **Start Update Window** and the **End Update Window**, if a Connector calls home to pick up a policy, it will pick up the product update. Because the Connector calls home at an interval dependent on the Heartbeat Interval, you will want to plan your Update Window accordingly: that is, ensure the interval specified in the Update Window is larger than the Heartbeat Interval.

File Tab

The File tab contains settings for the file scanning engine behaviors of your AMP for Endpoints Connectors, such as which engines to use, setting up scheduled scans, and cache settings.

File > Modes



File Conviction Mode allows you to specify the action the Connector takes when a malicious file is convicted. Setting this to **Audit** will stop the AMP for Endpoints Connector from quarantining any files.

WARNING! When **File Conviction Mode** is set to **Audit**, any malicious files on your endpoints will remain accessible and be allowed to execute. Application blocking lists will also not be enforced. You should only use this setting for testing purposes with proprietary software.

Monitor File Copies and Moves allows the AMP for Endpoints Connector to give real-time protection to files that are copied or moved.

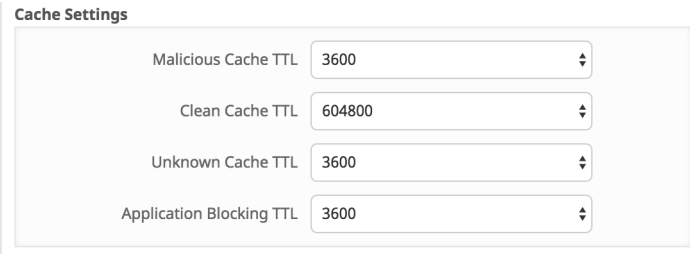
Monitor Process Execution allows the AMP for Endpoints Connector to give real-time protection to files that are executed.

On Execute Mode can run in two different modes: **Active** or **Passive**. In Active mode, the file is blocked from being executed until a determination of whether or not a file is malicious or a timeout is reached. In Passive mode, the file is allowed to be executed and in parallel the file is looked up to determine whether or not it is malicious. Although Active mode gives you better protection, it can cause performance issues and if the endpoint already has an antivirus product installed it is best to leave these set to Passive.

Maximum Scan File Size limits the size of files that are scanned by the AMP for Endpoints Connector. Any file larger than the threshold set will not be scanned.

Maximum Archive Scan File Size limits the size of archive files that are scanned by the AMP for Endpoints Connector. Any archive file larger than the threshold set will not be scanned.

File > Cache Settings



SHA-256 values are cached to reduce cloud lookup traffic. The amount of time a value is cached depends on the disposition of the file the last time a cloud lookup was performed on its SHA-256. While a file is cached, the Connector will always consider its disposition to be what it was the last time a cloud lookup was performed. For example, if a SHA-256 is in an application blocking list and the TTL is 3600 seconds, that application will continue to be blocked from execution by the Connector for the next hour even if the administrator removes it from the application blocking list.

Malicious Cache TTL is the time in seconds for which a file with a malicious disposition is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

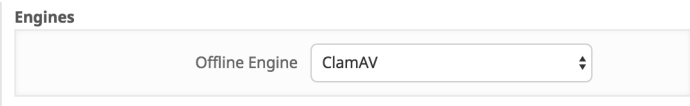
Clean Cache TTL is the time in seconds for which a file with a clean disposition is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 7 days.

Unknown Cache TTL is the time in seconds for which a file with an unknown disposition is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

Application Blocking TTL is the time in seconds for which a file that is in an Application Control - Blocking list is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

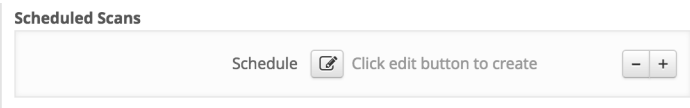
IMPORTANT! If you add a SHA-256 with a clean disposition that was previously seen by a Connector to an application blocking list, you must stop the Connector and delete the cloud_cache.db file from the installation directory on that computer for the application to be blocked from executing. Otherwise, you will have to wait until the TTL for the clean file expires and another cloud lookup is performed by the Connector before the application is blocked from executing.

File > Engines



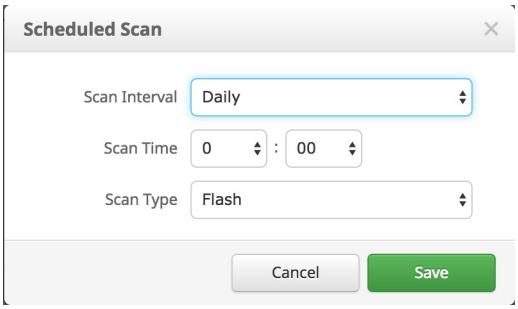
Offline Engine can be set to **Disabled** or **ClamAV**. ClamAV is a full antivirus product and should never be enabled if another antivirus engine is installed.

File > Scheduled Scans



Scheduled scans are not necessary for the operation of the AMP for Endpoints Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Retrospective. This allows companies to reduce their energy footprint by eliminating the need for scheduled scans. However, some companies may require scheduled scans due to policy so this can be enabled via policy when necessary.

When you click **Schedule**, an overlay will come up to allow you to choose the scan interval, time, and type.

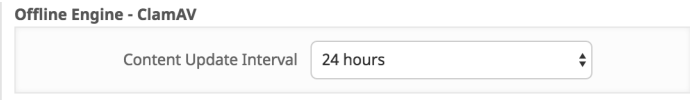


Scan Interval allows you to set how often the scan should run. The options are **Daily**, **Weekly**, or **Monthly**.

Scan Time allows you to set the time of day at which you want to commence the scan.

Scan Type allows you to set the type of scan. A **Flash** scan will scan the processes running and the files and registry entries used by those processes. A **Full** scan will scan the processes running, the registry entries, and all the files on disk. This scan is very resource-intensive and should not be performed on a regular basis. A **Custom** scan will scan a particular path that you give it.

File > Offline Engine - ClamAV



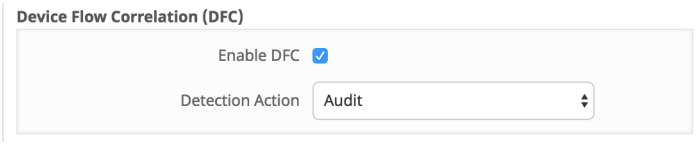
As a full antivirus product, ClamAV allows us to perform offline scanning. It is signature-based and will take up more disk space on the local computers. By default it will check for updated signatures every 24 hours and download them if new signatures are available. Its major draw back is compatibility with other antivirus products and should never be enabled if another antivirus product is installed on the computer. This policy configuration option is only available when ClamAV has been selected as the **Offline Engine** under **Engines**.

Content Update Interval allows you to specify how often your Connectors should check for new ClamAV content such as signatures. Longer update intervals will help to reduce network traffic caused by ClamAV updates, while shorter update intervals can consume significant bandwidth and is not recommended for large deployments.

Network Tab

The **Network** tab contains settings to for the network flow capabilities of your AMP for Endpoints Connectors, such as device flow correlation (DFC) settings.

Network > Device Flow Correlation (DFC)



Enable DFC will enable DFC on your AMP for Endpoints Connector. This allows you to monitor network activity and determine which action the Connector should take when connections to malicious hosts are detected.

Detection Action allows you to select whether the Connector will block network connections to malicious hosts or simply log them.

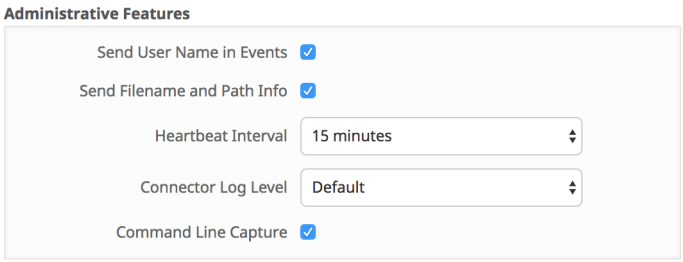
AMP for Endpoints Linux Policy

This section describes the policy options that are available for AMP for Endpoints Linux Connectors. The options are divided into three tabs: **General**, **File**, and **Network**.

General Tab

The **General** policy tab contains overall settings for your AMP for Endpoints Connectors such as proxy settings, update schedules, and general administrative settings.

General > Administrative Features



Send User Name in Events (available for AMP for Endpoints Linux Connector version 1.1.1 and later) will send the actual user name for which the process is executed, copied, or moved as if known. This is useful for tracking down who is seeing malware. If this is not enabled, you will see a "u" for malware executed, copied, or moved as a user and "a" for something executed copied or moved as an administrator.

Send Filename and Path Info will send the filename and path information to AMP for Endpoints so that they are visible in the **Events** tab, **Device Trajectory**, and **File Trajectory**. Unchecking this setting will stop this information from being sent.

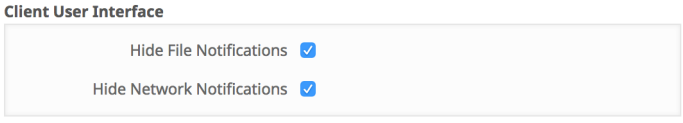
The **Heartbeat Interval** is the frequency with which the Connector calls home to see if there are any files to restore via Retrospective or by the administrator, any policies to pick up, or any tasks to perform such as product updates or scans.

Connector Log Level allows you to choose between default and debug (verbose) logging levels. The default level should be set unless debug is requested by support during troubleshooting.

Command Line Capture (AMP for Endpoints Linux 1.2 and higher) allows the Connector to capture command line arguments (including usernames, filenames, passwords, etc.) used during file execution and send the information to AMP for Endpoints. This information will be displayed in Device Trajectory for administrators as long as they have Two-Step Verification enabled.

If **Commmand Line Capture** is enabled, you can use **Command Line Logging** to log captured command line arguments to the local Connector log file (`/var/log/cisco`) on the endpoint. Note that the Command Line Logging setting only applies when the **Connector Log Level** setting is set to **Debug**.

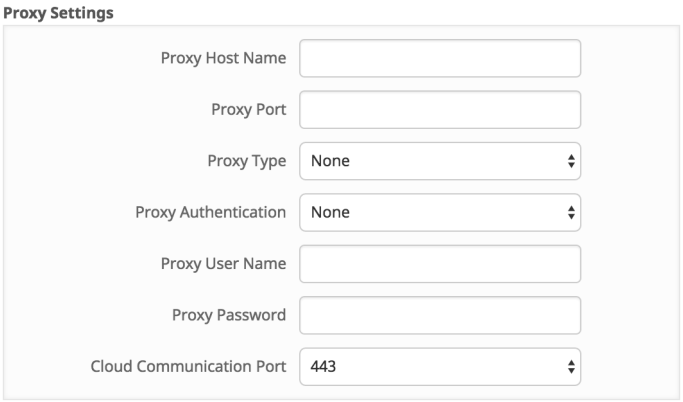
General > Client User Interface



Hide File Notifications suppresses notifications from being displayed to the command line interface when a malicious file is convicted or quarantined by the Connector.

Hide Network Notifications suppresses notifications from being displayed to the command line interface when a malicious network connection is detected or blocked by the Connector.

General > Proxy Settings



Proxy Hostname is the name or IP of the proxy server.

Proxy Port is the port on which the proxy server runs.

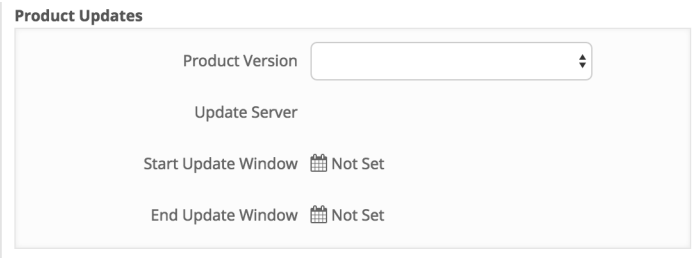
Proxy Type is the type of proxy you are connecting to. The Connector will support The Connector will support http_proxy, socks4, socks4a, socks5, and socks5_hostname.

Proxy Authentication is the type of authentication used by your proxy server. **Basic** and **NTLM** authentication are supported.

Proxy Username is used for authenticated proxies. This is the username you use to connect.

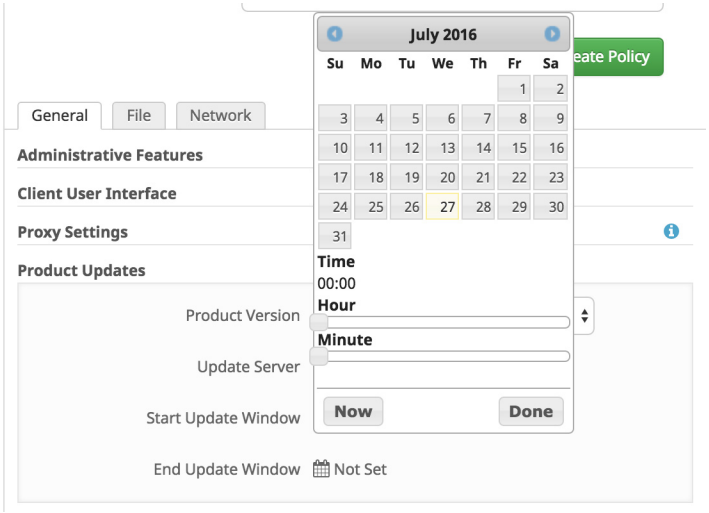
Proxy Password is used for authenticated proxies. This is the password you use with the proxy username.

General > Product Updates



When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** that shows which version you are going to; it will populate the **Update Server** so you can see where the files will be pulled from. You can then configure the **Start Update Window** and **End Update Window**.

The **Update Interval** allows you to specify how long your Connectors will wait between checks for new product updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic.



Start Update Window allows you to choose a date and time at which the updates can start occurring.

End Update Window allows you to choose a date and time at which the updates will stop occurring.

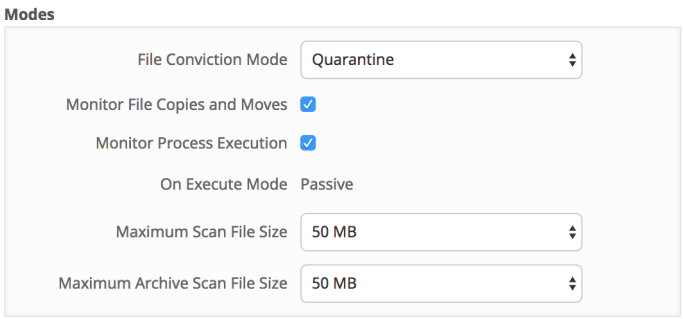
Between the **Start Update Window** and the **End Update Window**, if a Connector calls home to pick up a policy, it will pick up the product update. Because the Connector calls home at an interval that is dependent on the Heartbeat Interval, you will want to plan the update window accordingly; that is, make sure the interval specified in the Update Window is larger than the Heartbeat Interval.

IMPORTANT! To update the AMP for Endpoints Linux Connector via policy you must import the GPG Public Key to your RPM DB and have the `at` RPM installed with the `atd` service running. See Connector Updates for details.

File Tab

The **File** tab contains settings for the file scanning engine behaviors of your AMP for Endpoints Connectors such as which engines to use, setting up scheduled scans, and cache settings.

File > Modes



File Conviction Mode allows you to specify the action the Connector takes when a malicious file is convicted. Setting this to **Audit** will stop the Connector from quarantining any files.

WARNING! When **File Conviction Mode** is set to **Audit** any malicious files on your endpoints will remain accessible and be allowed to execute. Application blocking lists will also not be enforced. You should only use this setting for testing purposes with proprietary software.

Monitor File Copies and Moves is the ability for the Connector to give real-time protection to files that are copied or moved.

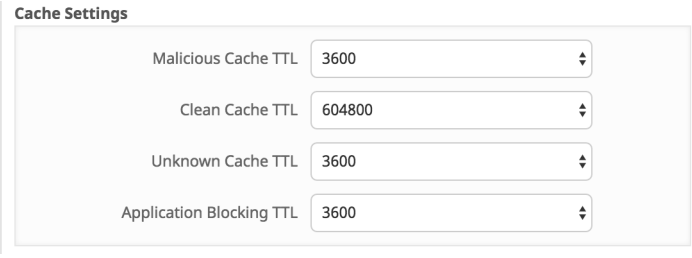
Monitor Process Execution is the ability for the Connector to give real-time protection to files that are executed.

On Execute Mode can only run in passive mode on AMP for Endpoints Linux. The file is allowed to be executed and in parallel the file is looked up to determine whether or not it is malicious.

Maximum Scan File Size limits the size of files that are scanned by the AMP for Endpoints Connector. Any file larger than the threshold set will not be scanned.

Maximum Archive Scan File Size limits the size of archive files that are scanned by the AMP for Endpoints Connector. Any archive file larger than the threshold set will not be scanned.

File > Cache Settings



SHA-256 values are cached to reduce cloud lookup traffic. The amount of time a value is cached depends on the disposition of the file the last time a cloud lookup was performed on its

SHA-256. While a file is cached, the Connector will always consider its disposition to be what it was the last time a cloud lookup was performed.

For example, if a SHA-256 is included in an application blocking list and the TTL is 3600 seconds, that application will continue to be blocked from execution by the Connector for the next hour even if the administrator removes it from the application blocking list.

Malicious Cache TTL is the time in seconds for which a file with a malicious disposition will be cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

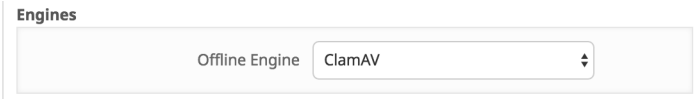
Clean Cache TTL is the time in seconds for which a file with a clean disposition will be cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 7 days.

Unknown Cache TTL is the time in seconds for which a file with an unknown disposition will be cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

Application Blocking TTL is the time in seconds for which a file that is in an application blocking list will be cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is 1 hour.

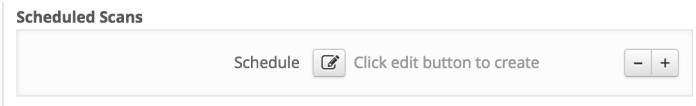
IMPORTANT! If you add a SHA-256 with a clean disposition that was previously seen by a Connector to an application blocking list, you must stop the Connector and delete the cache.db file from the installation directory on that computer for the application to be blocked from executing. Otherwise, you will have to wait until the TTL for the clean file expires and another cloud lookup is performed by the Connector before the application is blocked from executing.

File > Engines



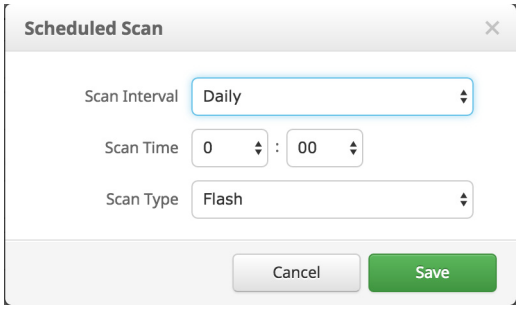
Offline Engine can be set to **Disabled** or **ClamAV**. ClamAV is a full antivirus product and should never be enabled if another antivirus engine is installed.

File > Scheduled Scans



Scheduled scans are not necessary for the operation of the Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Retrospective. This allows companies to reduce their energy footprint by eliminating the need for scheduled scans. However, some companies may require scheduled scans due to policy so this can be enabled via policy when necessary.

When you click the edit icon, an overlay will come up to allow you to choose the scan interval, time, and type.

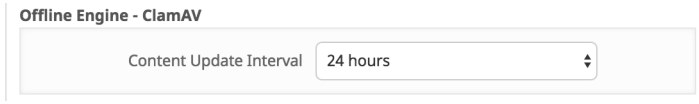


Scan Interval allows you to set how often the scan should run. The options are daily, weekly, or monthly.

Scan Time allows you to set the time of day at which you want to start the scan.

Scan Type allows you to set the type of scan. A **Flash** scan will scan the processes running, as well as the files and registry entries used by those processes. A **Full** scan will scan the processes running, as well as the registry entries, and all the files on disk. This scan is very resource-intensive and should not be performed on a regular basis. A **Custom** scan will only scan files on the path you provide.

File > Offline Engine - ClamAV



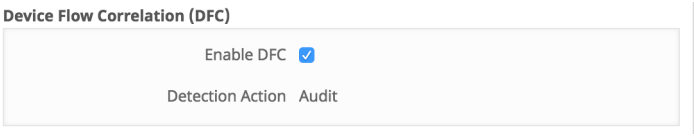
As a full antivirus product, ClamAV allows us to perform offline scanning. It is signature-based and will take up more disk space on the local computers. By default, it will check for updated signatures every 24 hours and download them if new signatures are available. Its major drawback is compatibility with other antivirus products: it should never be enabled if another antivirus product is installed on the computer. This policy configuration option is only available when ClamAV has been selected as the offline engine under **Engines**.

Content Update Interval lets you specify how often your Connectors should check for new ClamAV content, such as signatures. Longer update intervals will help to reduce network traffic caused by ClamAV updates, while shorter update intervals can consume significant bandwidth and are not recommended for large deployments.

Network Tab

The **Network** tab contains settings to for the network flow capabilities of your AMP for Endpoints Connectors such as device flow correlation (DFC) settings.

Network > Device Flow Correlation (DFC)

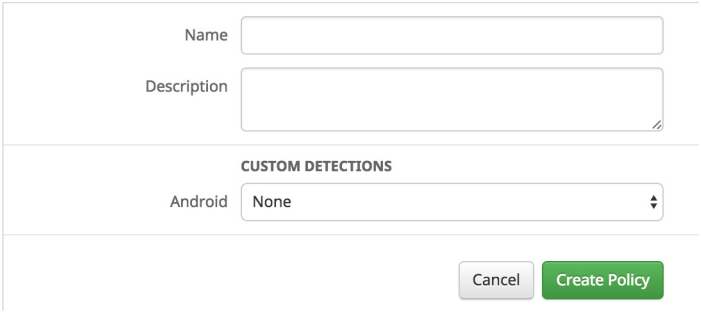


Enable DFC will enable DFC on your Connector. This allows you to monitor network activity and log any malicious activity.

Detection Action can only be set to **Audit** in order to log activity but not block it.

AMP for Endpoints Android Policy

A policy for the AMP for Endpoints Android Connector contains fewer options due to the nature of the device.

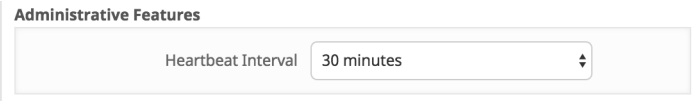


The **Name** is just the name that you designate to the policy. The Custom Detections - Android list type is described in the Outbreak Control section of this document. The **Description** can be used to give more information about the policy.

General Tab

The **General** policy tab contains overall settings for your AMP for Endpoints Connectors such as proxy settings, update schedules, and general administrative settings.

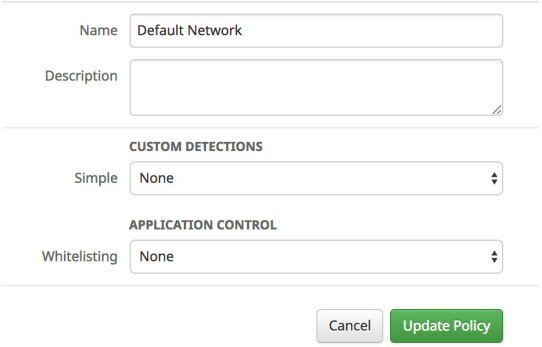
General > Administrative Features



The **Heartbeat Interval** is the frequency with which the Connector calls home to see if there are any policies to pick up, new custom detections or any tasks to perform such as product updates.

Network Policy

The Network policy is visible if Cisco Defense Center is integrated with AMP for Endpoints. For more information on Defense Center integration with AMP for Endpoints, see your Defense Center documentation.



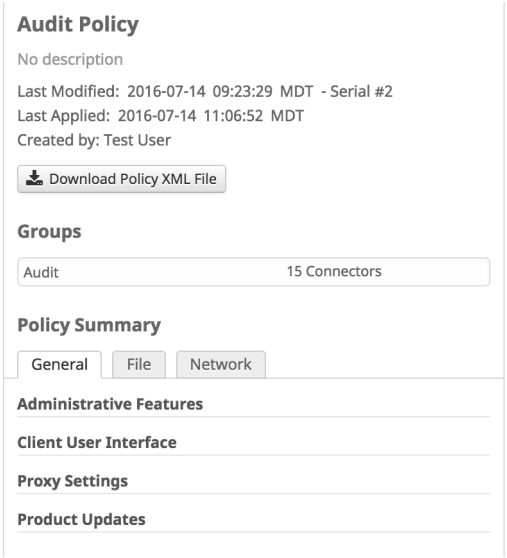
The **Name** is just the name that you designate to the policy. Custom detections are explained in the Outbreak Control section of this user guide. Whitelisting is explained in the Application Control - Whitelisting section. The **Description** can be used to give more information about the policy.

Policy Summary

Once you have created policies, you can view a summary of each policy's contents from the main **Policy Management** page. Click on the name of the policy you want to view and the summary will be displayed in the right-hand pane.

You can also download the XML file, which contains the specific policy for the AMP for Endpoints Connector using the **Download Policy XML File** button. The AMP for Endpoints

Connector installer contains the policy by default and this should only be used in specific troubleshooting scenarios.

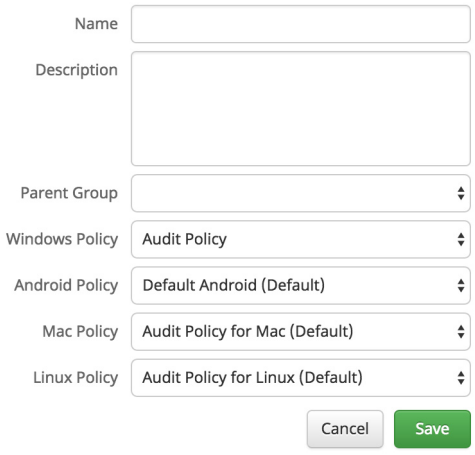


CHAPTER 6
GROUPS

Groups allow the computers in an organization to be managed according to their function, location, or other criteria that is determined by the administrator. To create a new group, click **Create Group**. You can also edit or delete existing groups. Use **View All Changes** to see a filtered view of the Audit Log, which shows all changes made to groups, or click **View Changes** on a specific group to see changes made only to that particular group.

Configuring the Group

This section will take you through the steps to create and configure the group. Creating a new group and editing an existing group follow the same procedure.



Name and Description

The name and description of the group are simply used to identify it. Groups can frequently reflect geographic locations, business units, user groups, and so on. Groups should be defined according to policies that will be applied to each one.

Parent Menu

The **Parent** menu allows you to set a parent group for the group you are creating. Because this is the first group being created on this particular AMP for Endpoints deployment the only options available are no parent group (a blank entry) or the Default Group.

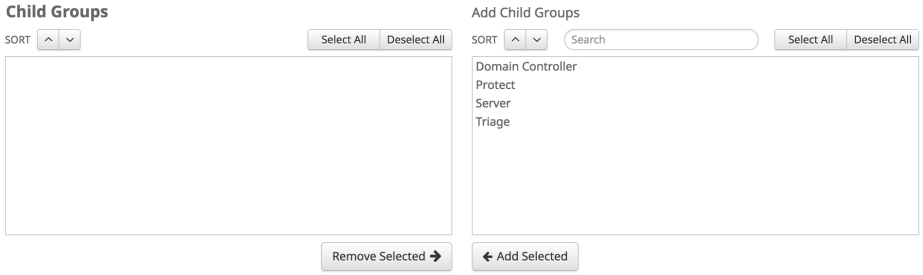
Policy Menu

The **Policy** menu allows you to specify which policy to apply to the group you are creating. By default, the Default Policy will be applied to the new group unless a parent group has been selected. If a parent has been selected, then the new group will inherit the policy of the parent.

IMPORTANT! If the parent group is changed later on, then the group will inherit the policy of its new parent group. If the parent group is deleted, then all child groups will be moved to the default group and inherit that policy.

Child Groups

You can also choose to add or remove any child groups to the current group. You can select individual groups, select multiple groups, or select all the groups, and make them child groups. You can also remove any child groups using the same methods.



IMPORTANT! If you remove a child group that inherits its policy from its parent, then that group's policy will revert to the business default policy until you assign it to a new parent group.

Adding and Moving Computers

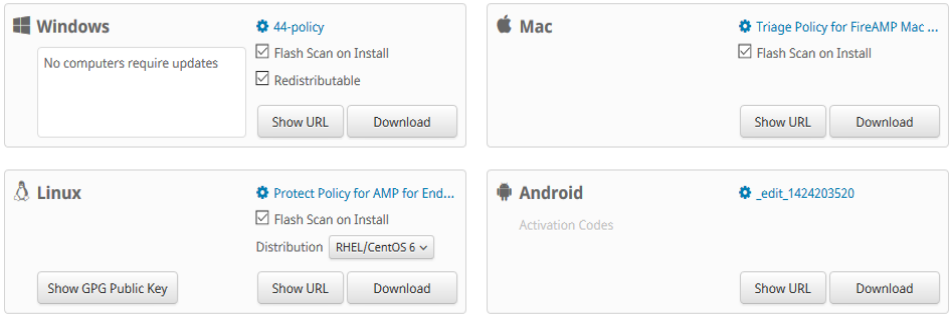
To assign computers to the new group, click **Save** then go to **Management > Computers** to add or move computers. See Computer Management for details.

CHAPTER 7
DEPLOYING THE AMP FOR ENDPOINTS CONNECTOR

After you have created policies and assigned them to groups, you can begin deploying the AMP for Endpoints Connector to computers and devices in your organization.

Download Connector

The **Download Connector** page allows you to download installer packages for each type of AMP for Endpoints Connector or copy the URL from which they can be downloaded. The installer package can be placed on a network share or distributed via management software. The download URL can be emailed to users to allow them to download and install it themselves, which can be convenient for remote users.



AMP for Endpoints Windows Connector

To deploy the AMP for Endpoints Windows Connector, first select a group from the drop-down menu. You will be able to see which Connectors in the group require an update to the version of the Connector you are downloading. It will also show how many of the computers will require a reboot when they are updated to the current version of Connector.

Choose whether to have the Connector perform a flash scan during the install process. The flash scan checks processes that are currently running in memory and should be performed on each install.

By default, you will download a redistributable installer. This is a 46 MB file that contains both the 32- and 64-bit installers. In order to install the AMP for Endpoints Connector on multiple computers, you can place this file on a network share or push it to all the computers in a group using a tool like System Center Configuration Manager. The installer contains a policy.xml file that is used as a configuration file for the install.

IMPORTANT! When using Microsoft System Center Configuration Manager (SCCM) to deploy the Connector to Windows XP computers, you must perform an additional step. Right-click on the AMP for Endpoints Connector installer and select **Properties** from the context menu. Under the **Environment** tab, check the **Allow users to interact with this program** box and click OK.

You can also choose to download a small (~900 KB) bootstrapper file to install the AMP for Endpoints Connector. This executable determines if the computer is running a 32- or 64- bit operating system and downloads and installs the appropriate version of the AMP for Endpoints Connector. Note that since the bootstrapper has to retrieve the main installer, it will not work from behind a proxy. You will have to use the redistributable installer instead.

IMPORTANT! On Windows XP and Windows Server 2003, if you have migrated the AMP for Endpoints Windows Connector to cisco.com addresses for connectivity, the bootstrapper will not work. You must download the redistributable installer for those operating system versions.

AMP for Endpoints Mac Connector

To deploy the AMP for Endpoints Mac Connector, first select a group from the drop-down menu. Choose whether to have the Connector perform a flash scan during the install process. The flash scan checks processes currently running in memory and should be performed on each install.

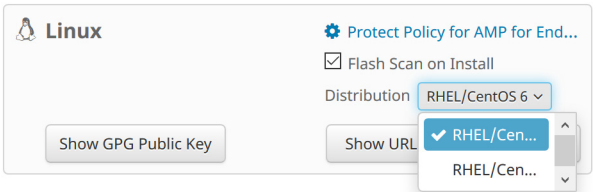
You can then download the PKG file to install the AMP for Endpoints Mac Connector or copy the download link. The installer is approximately 5 MB and can be placed on a network share. The PKG file also contains a policy.xml file that is used as a configuration file for the install.

AMP for Endpoints Linux Connector

To deploy the AMP for Endpoints Linux Connector first select a group from the drop down menu. Choose whether to have the Connector perform a flash scan during the install process. The flash scan checks processes currently running in memory and should be performed on each install.

You can then download the rpm file to install the AMP for Endpoints Linux Connector or copy the download link. The installer is approximately 16 MB and can be placed on a network share. The rpm file also contains a policy.xml file that is used as a configuration file for the install.

Download Connector allows you to select for either Red Hat Enterprise Linux (RHEL) or CentOS version 6.x or 7.x. Click on the **Distribution** pull-down to select either RHEL/CentOS 6 or RHEL/CentOS 7, as appropriate.



You should also copy or download the GPG Public Key linked on the download page. This will be required for Connector Updates via policy.

AMP for Endpoints Android Connector

The AMP for Endpoints Android Connector can be deployed by downloading the app or emailing a link to the app download to users. When the app is installed on a mobile device, an Activation Code will need to be entered.

To deploy the AMP for Endpoints Android Connector, you can download the APK file or copy the download link. Alternatively, you can also download the AMP for Endpoints Android Connector from the Google Play store.

Activation Codes

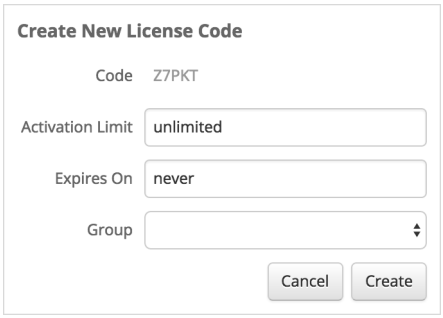
The **Activation Codes** screen allows you to generate activation codes required during AMP for Endpoints Android Connector installation on a device. To generate a new activation code, click **Create.**

Select the limit for the number of activations that can be performed using this code by entering the value in the **Activation Limit** field. By default, the value is set to unlimited. Next, choose the expiry date for the code using the calendar pull-down.

IMPORTANT! After the expiration date, new AMP for Endpoints Android Connectors cannot be activated using the code, but AMP for Endpoints Android Connectors that were activated using the code prior to the date will continue to function as normal.

By default, activation codes are set to never expire. Finally, select the group the activation code will be used by. Only one activation code can be applied to a group at a time, so make sure you

have assigned a high enough activation limit for the number of devices in the group you are applying the code to. Click **Create** to create the new activation code.

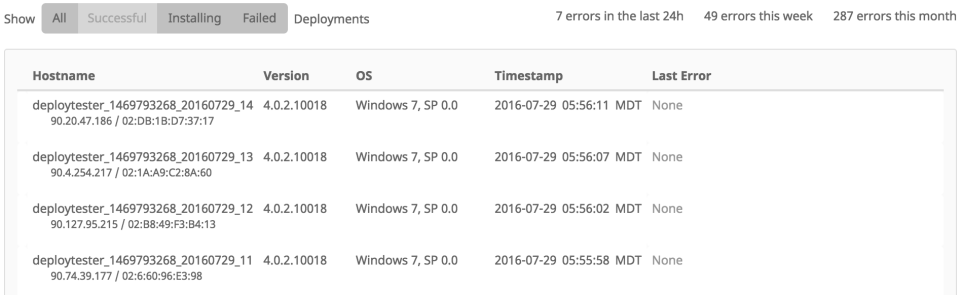


At any time you can change the settings for an activation code by clicking the **Edit** link next to its entry. You can also remove an activation code by clicking the **Delete** link next to its entry.

IMPORTANT! When you delete an activation code, all AMP for Endpoints Android Connectors that have been previously activated with that code will continue to function, but new AMP for Endpoints Android Connectors cannot be activated using that code.

Deployment Summary

The **Deployment Summary** page gives you a list of the successful and failed AMP for Endpoints Connector installs, as well as those currently in progress.



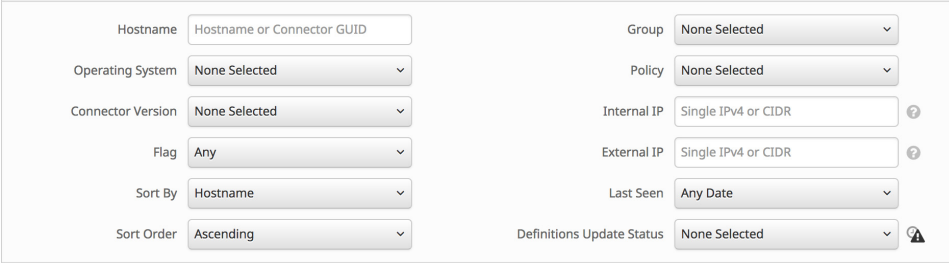
You can view the name of the computer, its IP address, its MAC address, and the date and time of the install attempt, as well as the operating system version and the AMP for Endpoints Connector version. In some cases, the install may have failed completely and a reason will be given for that, but in others there may not have been any further communication with the cloud after the install started.

Computer Management

After you have deployed the AMP for Endpoints Connector, the installed-on endpoints will begin to appear on the **Computers** screen, which is accessible from **Management > Computers**.The computer list shows all the endpoints that have installed the AMP for Endpoints Connector. **View All Changes** will take you to a filtered view of the Audit Log,

which shows all changes made to computers. You can apply filters to the list or navigate through the pages to view more computers. You can use the check boxes to select either all computers or specific computers in order to move them to another group, a new group, or to delete them. To download a list of computers including Connector GUID, hostname, operating system, Connector version, group, Connector install date, and the last seen date, and definitions update status, select one or more computers and click **Export to CSV**.

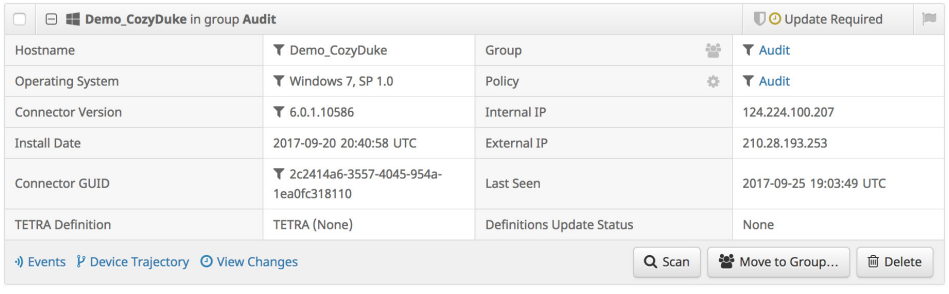
IMPORTANT! All dates and times in the exported CSV file will be in UTC regardless of your Time Zone Settings.



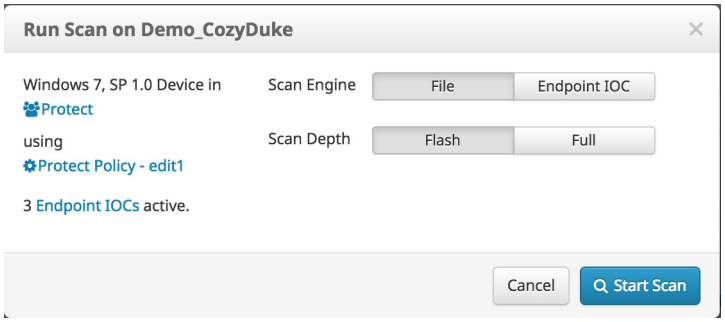
Clicking on a computer in the list will expand details of that computer. Clicking the + or - buttons will expand or collapse the details for every computer on the current page. From the details, you can change the Groups the computer belongs to, see which Policies apply to it, along with other information about the computer. Note that the Last Seen time is accurate within an approximately15-minute range. You can also delete the computer from the list, and flag or unflag the computer in the list. **View Changes** will take you to a filtered view of the Audit Log, which shows all changes for the specific computer.

IMPORTANT! Clicking the Last Seen time will display a popup with details, options to copy the time to the clipboard in ISO-8601 Date and UNIX Timestamp formats, and a link to change the time zone.

IMPORTANT! Deleting a computer will only remove it from appearing in the Computer Management page listing. Unless you uninstall the AMP for Endpoints Connector from the computer you will still see events generated by a deleted computer.

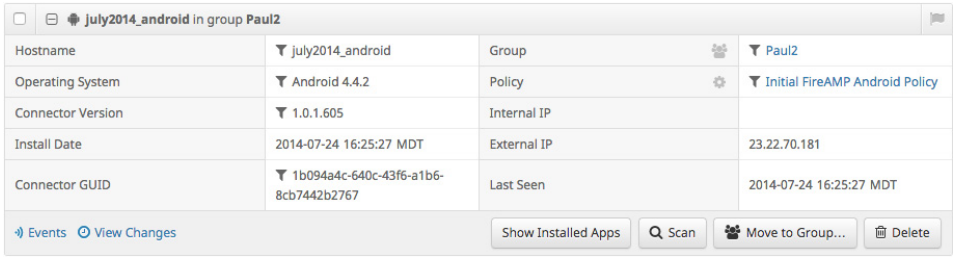


If you click **Scan**, a dialog will be displayed that allows you to select a file scan or IOC Scan, and whether to run a full or flash scan.

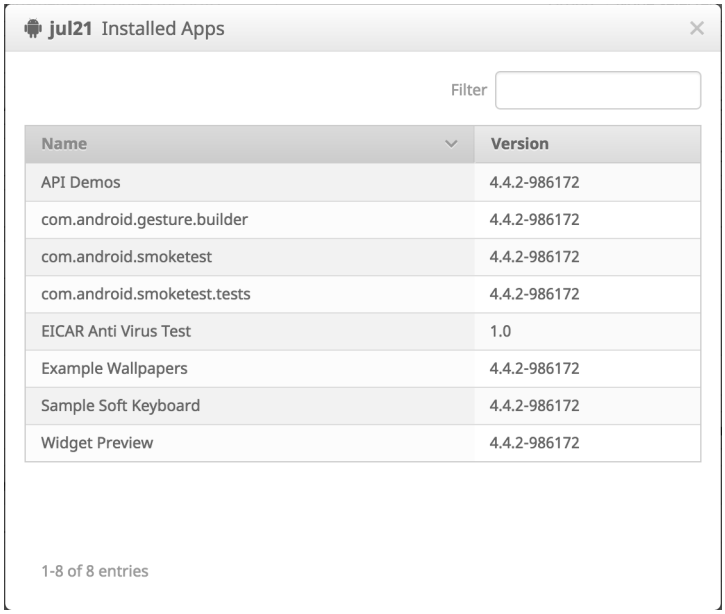


WARNING! Running a full Endpoint IOC scan is time consuming and resource intensive. On endpoints with a large number of files, a full scan can take multiple days to run. You should only schedule full scans during periods of inactivity, such as at night or on weekends. The first time you run a full scan on a Connector, the system will be cataloged, which will take longer than a regular full scan.

You can also click the **Browse events for this computer** button to open a filtered Events Tab view for the selected computer. For Android devices you also have the ability to view a list of installed applications for each device.



Click **Show Installed Apps** to view the list for a particular Android device.



CHAPTER 8
AMP FOR ENDPOINTS WINDOWS CONNECTOR

After you have defined groups, policies, and a deployment strategy, the AMP for Endpoints Connector can be installed on the endpoints. This section will go through the manual install process and highlight some of the key features of the Connector user interface.

System Requirements

The following are the minimum system requirements for the AMP for Endpoints Connector based on the operating system. The AMP for Endpoints Connector supports both 32-bit and 64-bit versions of these operating systems. Additional disk space may be required when enabling certain Connector features.

Microsoft Windows XP with Service Pack 3 or later

- 500 MHz or faster processor
- 256 MB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Microsoft Windows Vista with Service Pack 2 or later

- 1 GHz or faster processor
- 512 MB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Microsoft Windows 7

- 1 GHz or faster processor
- 1 GB RAM
- 650 MB available hard disk space - Cloud-only mode

- 1 GB available hard disk space - TETRA

Microsoft Windows 8 and 8.1 (requires AMP for Endpoints Connector 3.1.4 or later)

- 1 GHz or faster processor
- 512 MB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Microsoft Windows 10 (requires AMP for Endpoints Connector 4.3.0 or later)

- 1 GHz or faster processor
- 1 GB RAM (32-bit) or 2 GB RAM (64-bit)
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Microsoft Windows Server 2003

- 1 GHz or faster processor
- 512 MB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

Microsoft Windows Server 2008

- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space – Cloud only mode
- 1 GB available hard disk space – TETRA

Microsoft Windows Server 2012 (requires AMP for Endpoints Connector 3.1.9 or later)

- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space - Cloud only mode
- 1 GB available hard disk space - TETRA

Incompatible software and configurations

The AMP for Endpoints Windows Connector is currently not compatible with the following software:

- ZoneAlarm by Check Point
- Carbon Black
- Res Software AppGuard

The AMP for Endpoints Windows Connector does not currently support the following proxy configurations:

- Websense NTLM credential caching. The currently supported workaround for AMP for Endpoints is either to disable NTLM credential caching in Websense or allow the AMP for Endpoints Connector to bypass proxy authentication through the use of authentication exceptions.
- HTTPS content inspection. The currently supported workaround is either to disable HTTPS content inspection or set up exclusions for the AMP for Endpoints Connector.
- Kerberos / GSSAPI authentication. The currently supported workaround is to use either Basic or NTLM authentication.

Firewall Connectivity

To allow the AMP for Endpoints Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world.

IMPORTANT! If your firewall requires IP address exceptions, see this Cisco TechNote.

Firewall Exceptions

The firewall must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.immunet.com
- **Endpoint IOC Downloads** - ioc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - rff.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443:

- **Cloud Host** - cloud-ec.amp.cisco.com

For AMP for Endpoints Windows version 5.0 and higher you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.amp.cisco.com

If you have TETRA enabled on any of your AMP for Endpoints Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - update.amp.cisco.com

European Union Firewall Exceptions

Companies located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **Event Server** - intake.eu.amp.cisco.com
- **Management Server** - mgmt.eu.amp.cisco.com
- **Policy Server** - policy.eu.amp.cisco.com
- **Error Reporting** - crash.eu.amp.sourcefire.com
- **Endpoint IOC Downloads** - ioc.eu.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.eu.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - rff.eu.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.eu.amp.cisco.com

For AMP for Endpoints Windows version 5.0 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.eu.amp.cisco.com

If you have TETRA enabled on any of your AMP for Endpoints Connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - update.amp.cisco.com

Asia Pacific, Japan, and Greater China Firewall Exceptions

Companies located in the Asia Pacific, Japan, and Greater China region must allow connectivity from the Connector to the following servers over HTTPS:

- **Event Server** - intake.apjc.amp.cisco.com
- **Management Server** - mgmt.apjc.amp.cisco.com
- **Policy Server** - policy.apjc.amp.cisco.com
- **Error Reporting** - crash.apjc.amp.sourcefire.com
- **Endpoint IOC Downloads** - ioc.apjc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.apjc.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - rff.apjc.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.apjc.amp.cisco.com

For AMP for Endpoints Windows version 5.0 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.apjc.amp.cisco.com

If you have TETRA enabled on any of your AMP for Endpoints Connectors, you must allow access to the following server over TCP 80 for signature updates:

Update Server - update.amp.cisco.com

Proxy Autodetection

The Connector is able to use multiple mechanisms to support anonymous proxy servers. A specific proxy server or path to a proxy auto-config (PAC) file can be defined in Policies, or the Connector can discover the endpoint proxy settings from the Windows registry.

The AMP for Endpoints Connector can be set to discover endpoint proxy settings automatically. Once the Connector detects proxy setting information, it attempts to connect to the AMP for Endpoints Management Server to confirm that the proxy server settings are correct.

The Connector will first use the proxy settings specified in the policy. If the Connector is unable to establish a connection to the AMP for Endpoints Management Server it will attempt to retrieve proxy settings from the Windows registry on the endpoint. The Connector will attempt to retrieve the settings only from system-wide settings and not per-user settings.

If the Connector is unable to retrieve proxy settings from the Windows registry, it attempts to locate the proxy auto-configuration (PAC) file. This can be specified in policy settings or determined using Web Proxy Auto-Discovery protocol (WPAD). If the PAC file location is specified in policy, it has to begin with http or https. Note that PAC files supported are only ECMAScript-based and must have a .pac file extension. If the PAC file is hosted on a Web server, the proper MIME type of application/x-javascript-config must be specified.Since all Connector communications are already encrypted, https proxy is not supported. For version 3.0.6 of the Connector, a socks proxy setting cannot be specified using a PAC file.

The Connector will attempt to rediscover proxy settings after a certain number of cloud lookups fail. This is to ensure that when laptops are outside of the enterprise network, the Connector is able to connect when network proxy settings are changed.

Installer

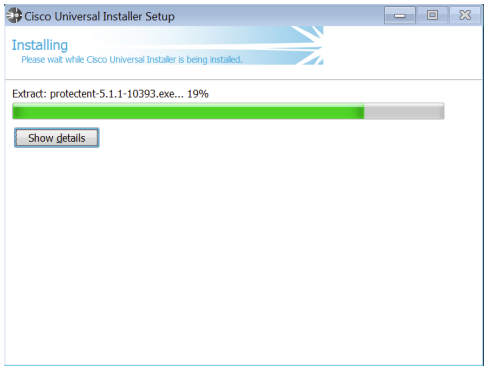
The installer can be run in either Interactive mode or using a series of command line parameters.

Interactive Installer

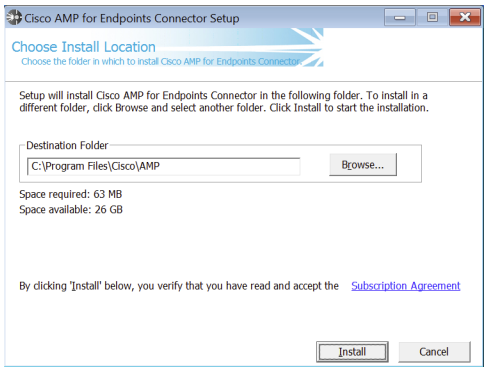
When installing via the bootstrapper, either as a downloaded file or via email, there will be interaction required on the endpoint unless the administrator has used the Installer Command Line Switches to perform a silent install and specify options.

If Windows User Access Control (UAC) is enabled, the user will be presented with a prompt. Click on **Yes** to continue.

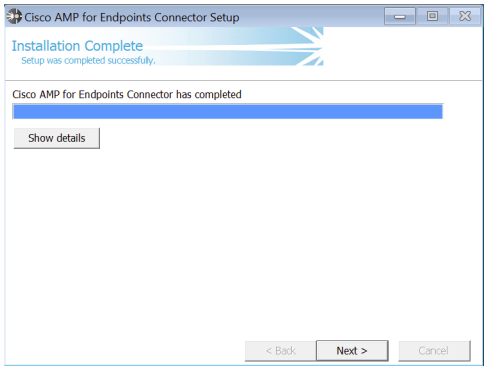
At this point the Download Manager will fetch the appropriate version of the installer package if installing through the bootstrapper. If the redistributable installer is used then this step will be skipped.



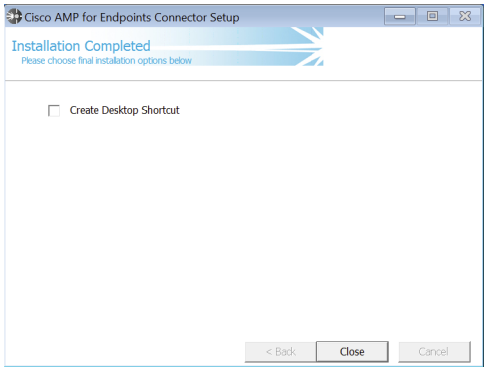
Next, the user is presented with the install location dialog. In most cases, the default location is the best choice. Links to the Connector End User License Agreement and Privacy Policy are also presented. Click **Install** to continue.



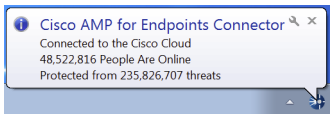
When the install is complete, click the **Next** button to continue.



The user can leave the box checked to have an icon for the Connector created on the desktop. Click the **Close** button to complete the install.



If the option to run a flash scan on install was selected, that scan will now execute. The Windows System Tray icon will also indicate that you are now connected to the Cisco Cloud if you selected Cloud Notifications in the policy applied to the Connector.



When the scan has completed, click **Close** to complete all install steps. The Connector will now be running on the endpoint.

Installer Command Line Switches

Administrators who have their own deployment software can use command line switches to automate the deployment. Here is a list of available switches:

- /R - For all Connector versions 5.1.13 and higher this must be the first switch used.

- /S - Used to put the installer into silent mode.

  IMPORTANT! This must be specified as the first parameter or the parameter immediately after /R.

- /desktopicon 0 - A desktop icon for the Connector will not be created.
- /desktopicon 1 - A desktop icon for the Connector will be created.
- /startmenu 0 - Start Menu shortcuts are not created.
- /startmenu 1 - Start Menu shortcuts are created.
- /contextmenu 0 - Disables Scan Now from the right-click context menu.
- /contextmenu 1 - Enables Scan Now in the right-click context menu.
- /remove 0 - Uninstalls the Connector but leaves files behind useful for reinstalling later.
- /remove 1 - Uninstalls the Connector and removes all associated files.
- /uninstallpassword [Connector Protection Password] – Allows you to uninstall the Connector when you have **Connector Protection** enabled in your policy. You must supply the **Connector Protection** password with this switch.
- /skipdfc 1 - Skip installation of the DFC driver.

  WARNING! Any Connectors installed using this flag must be in a group with a policy that has **Network > Device Flow Correlation (DFC) > Enable DFC** unchecked.

- /skiptetra 1 - Skip installation of the TETRA driver.

  WARNING! Any Connectors installed using this flag must be in a group with a policy that has **File > Engines > Offline Engine** set to **Disabled**.

- /D=[PATH] - Used to specify which directory to perform the install. For example, /D=C:\tmp will install into C:\tmp.

  IMPORTANT! This must be specified as the last parameter.

- /overridepolicy 1 - Replace existing policy.xml file when installing over a previous Connector install.
- /overridepolicy 0 - Do not replace existing policy.xml file when installing over a previous Connector install.
- /temppath - Used to specify the path to use for temporary files created during installation. For example, /temppath (c:\somepath\my temporary folder). This switch is only available in AMP for Endpoints Windows 5.0 and higher.

Running the command line installer without specifying any switches is equivalent to /desktopicon 0 /startmenu 1 /contextmenu 1 /skipdfc 0 /skiptetra 0 /overridepolicy 1.

There is a command line switch in AMP for Endpoints Windows Connector 5.1.3 and higher to enable users to opt in/out of migrating the install directory from "Sourcefire" to "Cisco" when upgrading from versions prior to 5.1.1 to versions 5.1.3 and higher. These are as follows:

- /renameinstalldir 1 will change the install directory from Sourcefire to Cisco.
- /renameinstalldir 0 will not change the install directory.

IMPORTANT! By default /renameinstalldir 1 will be used.

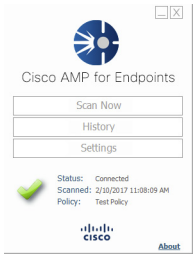
Installer Exit Codes

Administrators who use the command line switches to install the AMP for Endpoints Connector should be aware of the exit codes. They can be found in immpro_install.log in the %TEMP% folder.

- 0 – Success.
- 1500 – Installer already running.
- 1618 – Another installation is already in progress.
- 1633 – Unsupported Platform (i.e. installing 32 on 64 and vice versa).
- 1638 – This version or newer version of product already exists.
- 1801 – Invalid install path.
- 3010 – Success (Reboot required – will only be used on upgrade).
- 16001 – Your trial install has expired.
- 16002 – A reboot is pending on the users' system that must be completed before installing.
- 16003 – Unsupported Operating System (i.e. XP SP2, Win2000).
- 16004 – Invalid user permissions (not running as admin).
- 16005 - Existing AMP for Endpoints Connector service was already stopped or uses Connector Protection and the password was not supplied

Connector User Interface

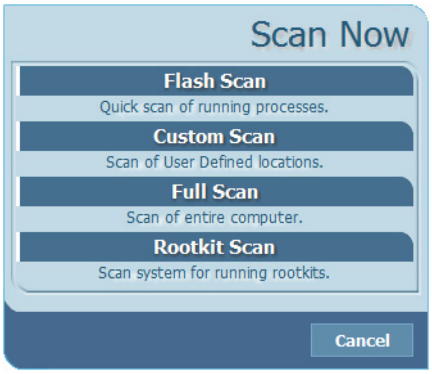
When the Connector is installed you can access it by double-clicking the desktop shortcut or clicking the **AMP for Endpoints Connector** entry in the Windows Start menu**.**



From the AMP for Endpoints Connector main screen you can choose to launch a scan, view the Connector history, or view the Connector settings. The Connector status is also shown, indicating whether it is connected to the network or if the service is stopped, when the last scan was performed, and the policy currently applied to the Connector. These entries can be useful in diagnosing Connector issues. The log file can be found in `%Program Files%\Cisco\AMP\[version number]\sfc.exe.log`.

Scanning

Click the **Scan Now** button to perform on demand scans with the Connector.



Available scanning options are:

Flash Scan: Scans the system registry and running processes for signs of malicious files. This scan is cloud-based and will require a network connection. The flash scan is relatively quick to perform.

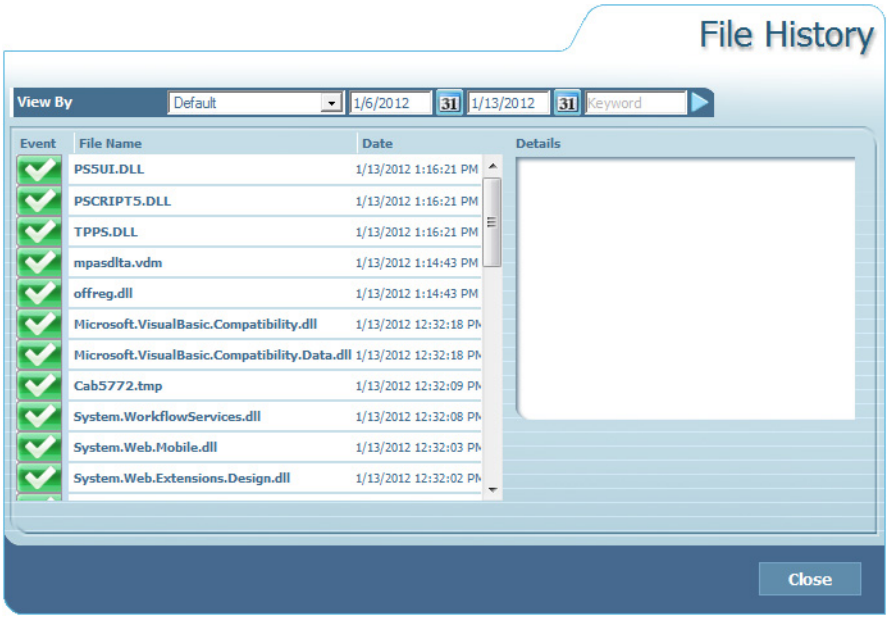
Custom Scan: Allows the user to define specific files or directories to scan. Selecting **Custom Scan** will open a dialog allowing the user to specify what should be scanned.

Full Scan: Scans the entire computer including all attached storage devices (such as USB drives). This scan can be time-consuming and resource-intensive, so should only be performed once when the Connector is first installed.

Rootkit Scan: This scans the computer for signs of installed rootkits. TETRA must be enabled in **Policy** to perform a rootkit scan, otherwise the **Rootkit Scan** button will be hidden.

History

The **History** pane allows you to view various file events that the Connector has been tracking.



There are different views available in **History**:

Default: All the data from the user in chronological order. Clicking on any file or event displays details in the right pane.

Clean File History: Lists all non-malicious files that have been downloaded to the computer in chronological order. Clean files are indicated by a green check mark next to the file name. Clicking on a file displays details in the right pane including the file path, the path and executable of the file that installed it, and the date the file was first seen by the Connector.

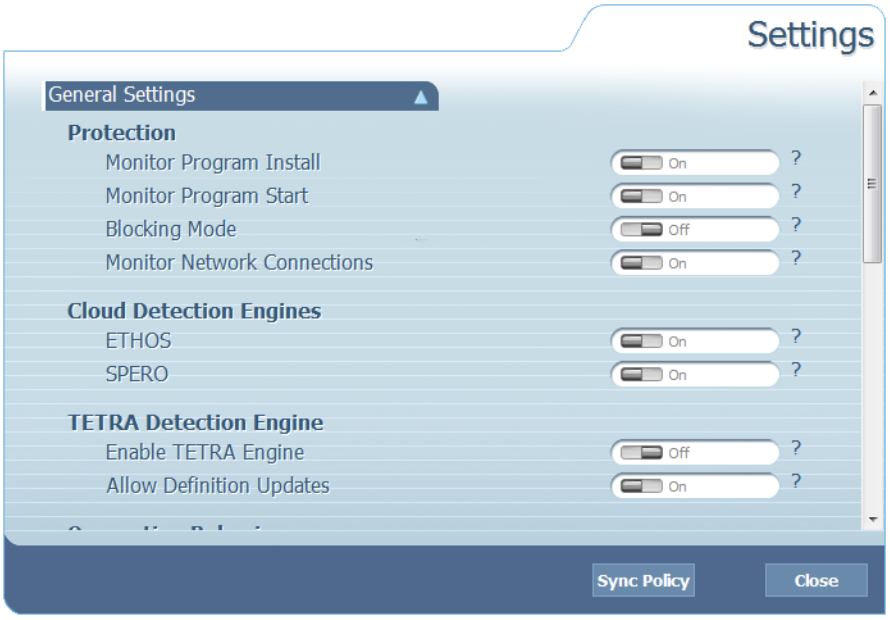
Malicious File History: Lists all detection and quarantine events associated with malicious files on the computer. Detections are indicated by a red X while successful quarantines are indicated by a red lock symbol next to the file names. Clicking on an event displays details in the right pane including the detection name, the path where the file was found, the path and executable of the file that installed it, and the date the event occurred.

Scan History: Details all scans performed by the Connector. Clicking on an event displays details in the right pane including the scan type, the result of the scan, and the date the scan was performed.

Settings

The **Settings** interface allows the individual user to see how the policy administrator has chosen to configure all aspects of the policy applied to the particular Connector. In a managed install, all the entries in the settings are read-only and are provided solely for informational and diagnostic purposes.

The **Sync Policy** button allows you to check for a policy update outside of the normal heartbeat interval. This is particularly useful during an outbreak situation where new custom detections have been added or if programs have been added or removed from whitelists and application blocking lists.



Support Tools

The AMP for Endpoints Windows Connector includes tools to assist in troubleshooting Connector issues.

Support Diagnostic Tool

The **Support Diagnostic** tool can be found in the Windows Start menu under the Cisco AMP for Endpoints Connector folder. Running the Support Diagnostic will create a snapshot and save it to the desktop as CiscoAMP_Support_Tool_[datetime].7z where [datetime] is the date and time the tool was run. You should only need to run this tool at the request of Cisco Support.

Timed Diagnostic Tool

The **Timed Diagnostic** tool can be found in the Windows Start menu under the Cisco AMP for Endpoints Connector folder. Running **Timed Diagnostic** will log activity for 30 minutes and save it to the desktop as CiscoAMP_Support_Tool_[datetime].7z where [datetime] is the date and time the tool was run. You should only need to run this tool at the request of Cisco Support.

Connectivity Test Tool

If any of your Connectors are having difficulty reaching the Cisco cloud you can use the Connectivity Test tool to assist in troubleshooting. It is available for version 5.1.1 and later of the AMP for Endpoints Windows Connector.

Open a command prompt using **Run as administrator** and navigate to the tool install folder. The tool is located in

```
%ProgramFiles%\Cisco\AMP\[Version]\ConnectivityTool.exe
```

where `[Version]` is the version number of the Connector, such as 5.1.1. You can run the tool with the /? switch to view a list of command line switches and what they do.

Switches include:

/D	Upload a crash dump test file to the Cisco cloud
/F[policynum]	Download a policy. If you specify a value for [policynum] then the tool will download this policy if it is a valid policy number.
/H	Perform an HTTP upload test to verify communication for the File Repository.
/I	Perform a connectivity test with the event intake server.
/J	Perform a connectivity test for console registration.
/T	Perform a connectivity test to a test URL to validate proxy settings. If this URL cannot be reached then the proxy settings are not saved to the configuration file.
/P[proxy]	Performs proxy detection. For [proxy] you can specify D to discover the proxy (default), P to retrieve proxy information from the policy.xml file, or - to bypass the proxy.
/V	Enable verbose logging mode.

If you run the tool without specifying any switches is runs as:

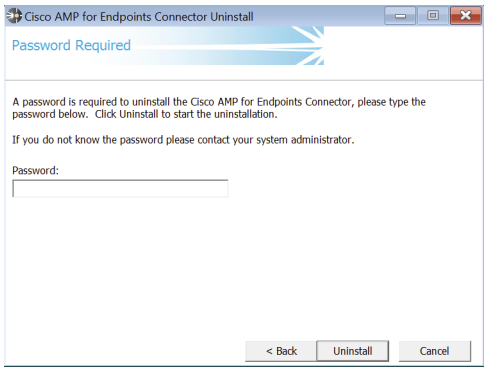
```
ConnectivityTool /D /F /H /I /J /T /PD
```

Each time you run the tool it will create a log file in the same directory with the file name ConnectivityTool.exe.log.

Uninstall

To uninstall a Connector from an endpoint, select **Control Panel** from the Start Menu. Under **Programs** select **Uninstall a program**. Select AMP for Endpoints Connector in the program list then click **Uninstall/Change**. Click the **Uninstall** button on the dialog box to remove the

application. If a password requirement to uninstall the Connector has been set in **Policy** you will be prompted to enter it.



When the uninstall process finishes click the **Close** button. Finally, you will be presented with a prompt asking if you want to delete all the AMP for Endpoints Connector history and quarantine files. Reboot the computer to complete the uninstall process.

IMPORTANT! On Windows 8 and higher, if **Fast Startup** mode is enabled, you should reboot the computer after uninstall is complete rather than using the Windows shutdown option. This will ensure that the final cleanup steps to remove the Connector drivers complete properly.

CHAPTER 9
AMP FOR ENDPOINTS MAC CONNECTOR

After you have defined groups, policies, and a deployment strategy, the AMP for Endpoints Connector can be installed on the endpoints. This section will go through the manual install process and highlight some of the key features of the Connector user interface.

System Requirements

The following are the minimum system requirements for the AMP for Endpoints Mac Connector based on the operating system. The AMP for Endpoints Mac Connector only supports 64-bit Macs.

Apple OS X 10.8

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.9

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.10 (requires AMP for Endpoints Mac Connector 1.0.6 or later)

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.11 (requires AMP for Endpoints Mac Connector 1.0.7 or later)

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.12 (requires AMP for Endpoints Mac Connector 1.2.4 or later)

- 2 GB RAM
- 65 MB available hard disk space

Apple OS X 10.13 (requires AMP for Endpoints Mac Connector 1.5.0 or later)

- 2 GB RAM
- 65 MB available hard disk space

Incompatible Software and Configurations

The AMP for Endpoints Mac Connector does not currently support the following proxy configurations:

- Websense NTLM credential caching: The currently supported workaround for AMP for Endpoints is either to disable NTLM credential caching in Websense or allow the AMP for Endpoints Connector to bypass proxy authentication through the use of authentication exceptions.
- HTTPS content inspection: The currently supported workaround is either to disable HTTPS content inspection or set up exclusions for the AMP for Endpoints Connector.
- Kerberos / GSSAPI authentication: The currently supported workaround is to use either Basic or NTLM authentication.

Firewall Connectivity

To allow the AMP for Endpoints Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are three sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world.

IMPORTANT! If your firewall requires IP address exceptions see this Cisco TechNote.

Firewall Exceptions

The firewall must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.immunet.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - rff.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.amp.cisco.com

For AMP for Endpoints Mac version 1.2 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.amp.cisco.com

If you have ClamAV enabled on any of your AMP for Endpoints Mac Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

European Union Firewall Exceptions

Organizations located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **Event Server** - intake.eu.amp.cisco.com
- **Management Server** - mgmt.eu.amp.cisco.com
- **Policy Server** - policy.eu.amp.cisco.com
- **Error Reporting** - crash.eu.amp.sourcefire.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - rff.eu.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.eu.amp.cisco.com

For AMP for Endpoints Mac version 1.2 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.eu.amp.cisco.com

If you have ClamAV enabled on any of your AMP for Endpoints Mac Connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

Asia Pacific, Japan, and Greater China Firewall Exceptions

Organizations located in the Asia Pacific, Japan and Greater China region must allow connectivity from the Connector to the following servers over HTTPS:

- **Event Server** - intake.apjc.amp.cisco.com
- **Management Server** - mgmt.apjc.amp.cisco.com
- **Policy Server** - policy.apjc.amp.cisco.com
- **Error Reporting** - crash.apjc.amp.sourcefire.com

- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - rff.apjc.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

- **Cloud Host** - cloud-ec.apjc.amp.cisco.com

For AMP for Endpoints Mac version 1.2 and higher, you will need to use the following Cloud Host address and enrollment server (both TCP 443) instead:

- **Cloud Host** - cloud-ec-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.apjc.amp.cisco.com

If you have ClamAV enabled on any of your AMP for Endpoints Mac Connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

Installing the AMP for Endpoints Mac Connector

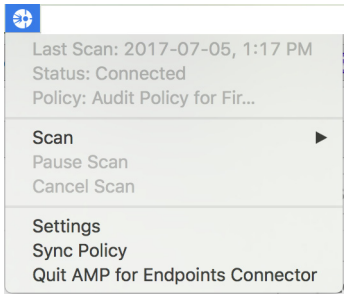
The AMP for Endpoints Mac Connector does not use a signed installer package; so rather than simply double-clicking on the pkg file, you have to right-click the pkg file and select **Open**. Alternatively, you can also install the pkg file from the terminal using the installer command. For more information, type `man installer` from the terminal. When prompted that the file is from an unidentified developer, click **Open** and you will be presented with the initial installer screen. Click **Continue** to proceed.

Read the software license agreement and click **Continue**. Click **Agree** to accept the terms of the agreement. Next, select the destination drive for the software installation. The Connector requires around 14 MB of free disk space and approximately 50 MB for signature files. Click **Continue** to proceed.

Once you are satisfied with the installation location, click **Install** to begin. You will be prompted for your password to continue. Once the installation is complete, you may be prompted about the application daemon accepting incoming network connections. Click **Allow** so that the Connector can receive updates from the Cisco cloud. Click **Finish** to complete the AMP for Endpoints Mac Connector installation.

Using the AMP for Endpoints Mac Connector

The AMP for Endpoints Mac Connector user interface is a menulet that appears on your Mac's menu bar.



The menulet primarily provides information such as when the last scan was performed, the current status, and the policy the Connector is using. You can also start, pause, and cancel scans from the menulet.

Sync Policy will check to make sure your Connector is running the most recent version of the policy. If not, it will download the latest version.

Versions 1.2 and higher of the AMP for Endpoints Mac Connector use a command line interface in addition to a graphical user interface on endpoints. The Connector command line interface can be found at `/opt/cisco/amp/ampcli` (`/usr/local/libexec/sourcefire/ampcli` for versions prior to 1.4.0). It can be run in interactive mode or execute a single command then exit. Use `./ampcli --help` to see a full list of options and commands available.

Settings

The **Settings** interface allows the individual user to see how the policy administrator has chosen to configure all aspects of the policy applied to the particular Connector. In a managed install, all the entries in the settings are read-only and provided solely for informational and diagnostic purposes.

Mail.app

Email messages containing malware will not be quarantined by the AMP for Endpoints Mac Connector to prevent corruption of the local mail database. Email messages will still be scanned and a detection event will be generated for any malware allowing the administrator to remove the malicious email directly from the mail server but a quarantine failed event will also appear. If Mail.app is configured to automatically download attachments, any malicious attachments will be quarantined as expected.

Uninstall

To uninstall the AMP for Endpoints Mac Connector, navigate to the installation folder **Applications** > **Cisco AMP** and double-click the **Uninstall AMP for Endpoints Connector.pkg** file. Follow the steps in the wizard to uninstall the application.

If for any reason the uninstaller is not successful, the AMP for Endpoints Mac Connector will have to be manually removed. To do this, open a terminal window and execute the following commands:

1. `/bin/launchctl unload /Library/LaunchAgents/com.cisco.amp.agent.plist`

   If this does not stop the menulet, click on it and select Quit AMP for Endpoints Connector.
2. `sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist`
3. `sudo /bin/launchctl list com.cisco.amp.daemon`

   This should yield the message: Could not find service.
4. `sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.updater.plist`
5. `sudo /bin/launchctl list com.cisco.amp.updater`

   This should yield the message: Could not find service "com.cisco.amp.updater" in domain for system.
6. `sudo /sbin/kextunload -b com.cisco.amp.fileop`
7. `sudo /sbin/kextunload -b com.cisco.amp.nke`
8. `sudo /usr/sbin/kextstat -l | grep com.cisco.amp`

   This should yield an empty list.
9. `sudo rm -rf "/Applications/Cisco AMP"`
10. `sudo rm -rf /Library/Extensions/ampfileop.kext`
11. `sudo rm -rf /Library/Extensions/ampnetworkflow.kext`
12. `sudo rm -rf "/Library/Application Support/Cisco/AMP for Endpoints Connector"`
13. `sudo rm -rf /opt/cisco/amp/`
14. `sudo rm -f /Library/Logs/Cisco/amp*`
15. `sudo rm -f /var/run/ampdaemon.pid`
16. `sudo rm -f /Library/LaunchAgents/com.cisco.amp.agent.plist`
17. `sudo rm -f /Library/LaunchDaemons/com.cisco.amp.daemon.plist`
18. `sudo rm -f /Library/LaunchDaemons/com.cisco.amp.updater.plist`
19. `sudo pkgutil --forget com.cisco.amp.agent`
20. `sudo pkgutil --forget com.cisco.amp.daemon`
21. `sudo pkgutil --forget com.cisco.amp.kextsigned`
22. `sudo pkgutil --forget com.cisco.amp.kextunsigned`

23. `sudo pkgutil --forget com.cisco.amp.support`
24. `sudo pkgutil --forget com.sourcefire.amp.agent`
25. `sudo pkgutil --forget com.sourcefire.amp.daemon`
26. `sudo pkgutil --forget com.sourcefire.amp.kextsigned`
27. `sudo pkgutil --forget com.sourcefire.amp.kextunsigned`
28. `sudo pkgutil --forget com.sourcefire.amp.support`
29. For each user: `rm -f ~/Library/Preferences/SourceFire-Inc.FireAMP-Mac.plist`
30. For each user: `rm -f ~/Library/Preferences/Cisco-Inc.AMP-for-Endpoints-Connector.plist`

CHAPTER 10
AMP FOR ENDPOINTS LINUX CONNECTOR

After you have defined groups, policies, and a deployment strategy, the AMP for Endpoints Connector can be installed on the endpoints. This section will go through the manual install process and highlight some of the key features of the Connector user interface.

System Requirements

The following are the minimum system requirements for the AMP for Endpoints Linux Connector based on the operating system. The AMP for Endpoints Linux Connector only supports x64 architectures.

CentOS 6.4/6.5/6.6/6.7/6.8/7.2/7.3

- 1 GB RAM
- 400 MB available hard disk space

Red Hat Enterprise Linux 6.5/6.6/6.7/6.8/7.2/7.3

- 1 GB RAM
- 400 MB available hard disk space

IMPORTANT! The AMP for Endpoints Linux Connector may not install properly on custom kernels. If you have a custom kernel, contact Support before attempting to install.

Incompatible software and configurations

The AMP for Endpoints Linux Connector is currently not compatible with the following software:

- F-Secure Linux Security
- Kaspersky Endpoint Security
- McAfee VSE for Linux
- McAfee Endpoint Security for Linux
- Sophos Server Security 9
- Symantec Endpoint Protection

The AMP for Endpoints Linux Connector may cause unmount failures with removable media or temporary file systems mounted in non-standard locations in Centos and Red Hat Enterprise Linux versions 6.x. In accordance with the File System Hierarchy Standard, removable media such as USB storage, DVDs, and CD-ROMs should be mounted to `/media/` while temporarily mounted file systems such as NFS file system mounts should be mounted to `/mnt/`. Mounting removable media or temporary file systems to other directories can cause a conflict where unmount fails due to device busy. Upon encountering an unmount failure, the user must stop the cisco-amp service, retry the unmount operation, then restart cisco-amp.

```
sudo initctl stop cisco-amp
sudo umount {dir\device}
sudo initctl start cisco-amp
```

The AMP for Endpoints Linux Connector does not support UEFI Secure Boot.

The AMP for Endpoints Linux Connector uses kernel modules that when loaded in Red Hat Enterprise Linux 7.x or CentOS 7.x taints the kernel. To temporarily prevent AMP from influencing kernel taint, the AMP service can be disabled, which prevents these kernel modules being loaded after the system restarts. This procedure should be used with caution, as disabling the AMP service effectively disables AMP protection on this system. To disable the AMP service, run the commands:

```
sudo systemctl disable cisco-amp
sudo systemctl stop cisco-amp
```

A system restart is required to reload the kernel and reset the kernel taint value. To re-enable the AMP service, run the commands:

```
sudo systemctl enable cisco-amp
sudo systemctl start cisco-amp
```

Firewall Connectivity

To allow the AMP for Endpoints Connector to communicate with Cisco cloud servers, the firewall must allow the clients to connect to certain servers over specific ports. There are three

sets of servers depending on where you are located: one for the European Union, one for Asia Pacific, Japan, and Greater China, and one for the rest of the world.

IMPORTANT! If your firewall requires IP address exceptions see this Cisco TechNote.

Firewall Exceptions

The firewall must allow connectivity from the Connector to the following servers over HTTPS (TCP 443):

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.immunet.com
- **Connector Upgrades** - upgrades.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following servers over TCP 443:

- **Cloud Host** - cloud-ec-asn.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.amp.cisco.com

If you have ClamAV enabled on any of your AMP for Endpoints Linux Connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

European Union Firewall Exceptions

Organizations located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **Event Server** - intake.eu.amp.cisco.com
- **Management Server** - mgmt.eu.amp.cisco.com
- **Policy Server** - policy.eu.amp.cisco.com
- **Error Reporting** - crash.eu.amp.sourcefire.com
- **Connector Upgrades** - upgrades.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups, the firewall must allow the clients to connect to the following servers over TCP 443:

- **Cloud Host** - cloud-ec-asn.eu.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.eu.amp.cisco.com

If you have ClamAV enabled on any of your AMP for Endpoints Linux Connectors, you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

Asia Pacific, Japan, and Greater China Firewall Exceptions

Organizations located in the European Union must allow connectivity from the Connector to the following servers over HTTPS:

- **Event Server** - intake.apjc.amp.cisco.com
- **Management Server** - mgmt.apjc.amp.cisco.com
- **Policy Server** - policy.apjc.amp.cisco.com
- **Error Reporting** - crash.apjc.amp.sourcefire.com
- **Connector Upgrades** - upgrades.amp.cisco.com

To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following servers over TCP 443:

- **Cloud Host** - cloud-ec-asn.apjc.amp.cisco.com
- **Enrollment Server** - cloud-ec-est.apjc.amp.cisco.com

If you have ClamAV enabled on any of your AMP for Endpoints Linux Connectors you must allow access to the following server over TCP 80 for signature updates:

- **Update Server** - defs.amp.sourcefire.com

Installing the AMP for Endpoints Linux Connector

To install the Connector execute the following command:

```
sudo yum localinstall [rpm package] -y
```

where `[rpm package]` is the name of the file, for example Audit_fireamplinux_connector.rpm.

Connector Updates

You can also copy the GPG Public Key from the Download Connector page to verify the signing of the RPM. The Connector can be installed without the GPG key, but if you plan on pushing Connector updates via policy you will need to import the GPG key into your RPM DB. You will also need the `at` RPM package installed with the `atd` service running.

To import the GPG key:

1. Verify the GPG key by clicking the GPG Public Key link on the Download Connector page. Compare the key to the one at `/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp`.
2. Run the following command from a terminal to import the key: `sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp`

3. Verify the key was installed by running the following command from a terminal: `rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'`
4. Look for a GPG key from Sourcefire in the output.

The Updater is run by the system's init daemon and when an update is available, automatically triggers the RPM upgrade process. Some SELinux configurations forbid this behavior and will cause the Updater to fail. If you suspect this is happening, examine the system's audit log (e.g., /var/log/audit/audit.log) and search for denial events related to ampupdater. You may need to adjust SELinux rules to allow Updater to function.

Using the AMP for Endpoints Linux Connector

The AMP for Endpoints Linux Connector uses a command line interface rather than a graphical user interface on endpoints. The AMP for Endpoints Linux Connector command line interface can be found at `/opt/cisco/amp/bin/ampcli`. It can be run in interactive mode or execute a single command then exit. Use `./ampcli --help` to see a full list of options and commands available. All log files generated by the Connector can be found in `/var/log/cisco`.

Support Tool

The support tool can be found at `/opt/cisco/amp/bin/ampsupport`. There are two ways to generate a support package:

```
sudo ./ampsupport
```

This will place the support package in the current user's desktop directory if it exists. Otherwise it will create the support package in the current user's home directory.

```
sudo ./ampsupport -o [path]
```

This will place the support package in the directory specified by [path]. For example, `sudo ./ampsupport -o /tmp` will place the file in /tmp.

Uninstall

To uninstall the AMP for Endpoints Linux Connector, execute the following command:

```
sudo yum remove ciscoampconnector -y
```

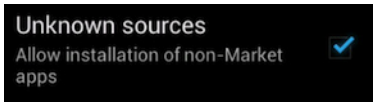
Note that this will leave behind local data including history and quarantined files if you plan on installing the Connector again. If you do not plan on reinstalling the Connector and want to remove the remaining files, run the following script:

```
/opt/cisco/amp/bin/purge_amp_local_data
```

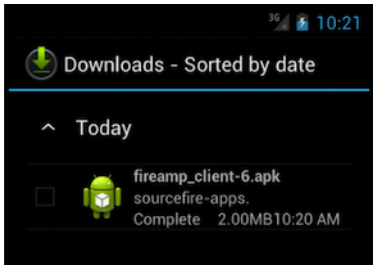
CHAPTER 11
AMP FOR ENDPOINTS ANDROID CONNECTOR

The AMP for Endpoints Android Connector requires Android 2.1 or higher running on ARM and Intel Atom processors with 4 MB of free space on the device.

Before the app can be installed, the user will have to allow installation of apps from non-Market sources on the device. To do this go to the device's **Settings** and select **Security**. Then check the box **Unknown sources**.



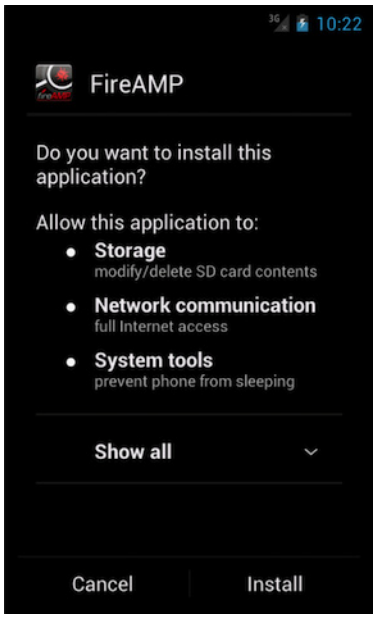
Once the fireamp_client.apk file has been downloaded it will be located in the device's **Downloads** folder.



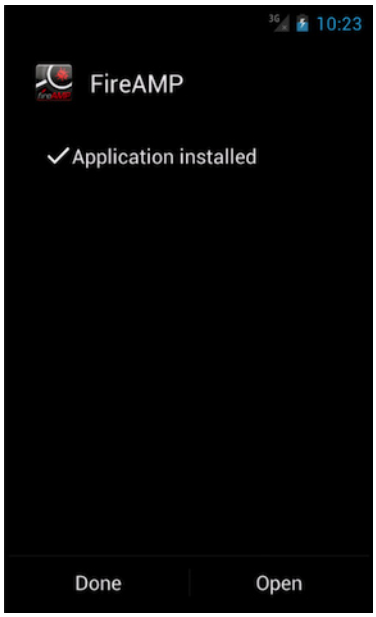
Simply tap the downloaded file to begin installation.

Installer

You will be prompted to review the permissions required before installation begins.



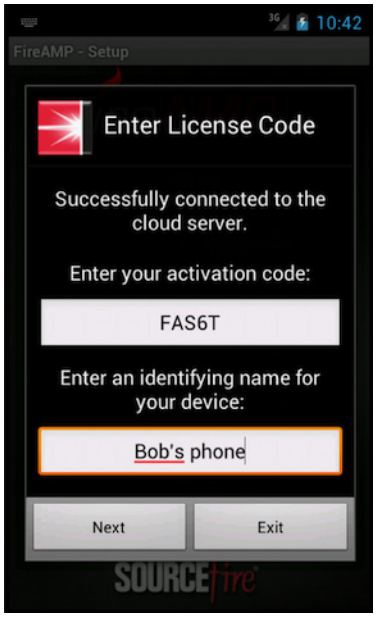
Once installation is complete, select **Open** to launch the application.



To agree to the license terms select **Accept**.

The AMP for Endpoints Android Connector will then attempt to establish a connection to the Cisco Cloud.

Enter the activation code for the phone, if necessary. In most cases, the activation code will already be populated before the install. Next, enter a name to identify the device in your Console. Select **Next** to continue.



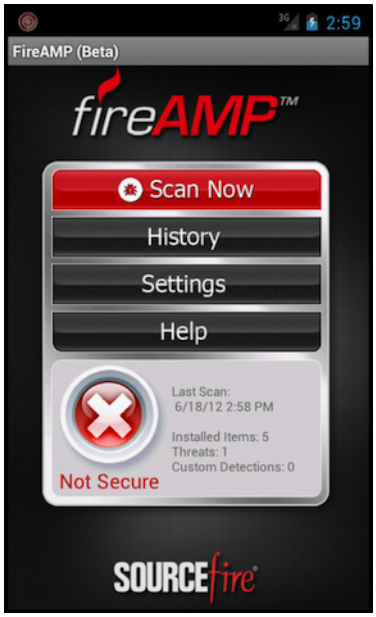
Select **Consent and Accept** to agree to the terms and consent to the use of the product on your device.

The application will begin an initial scan of the device for any malicious or non-compliant apps. If any are found either a yellow or red warning icon is displayed indicating that further action is required.

If no threats or non-compliant apps are detected a green check mark will indicate that the device is secure.

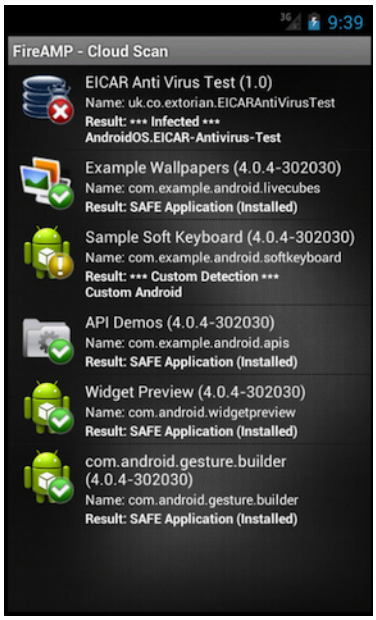
Removing Threats

If at any time a threat or non-compliant app is detected on the device, the user must take steps to remediate it. When a threat is detected, a notification will appear in the status bar. Further information can be viewed by expanding the notification center or opening the AMP for Endpoints Android app.

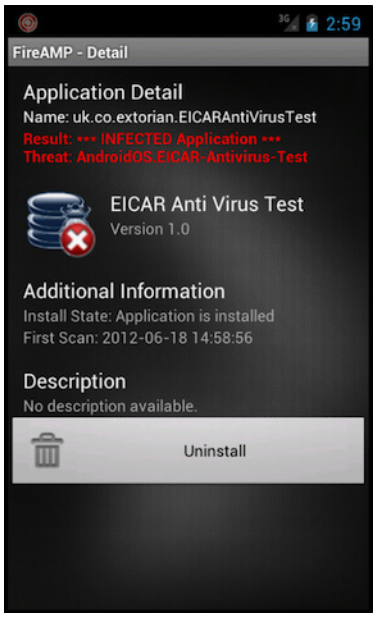


After a scan is completed, a summary is displayed that shows how many apps were scanned, how many of those apps were clean, the number that were malicious, and the number matching an entry in a Custom Detections - Android list.

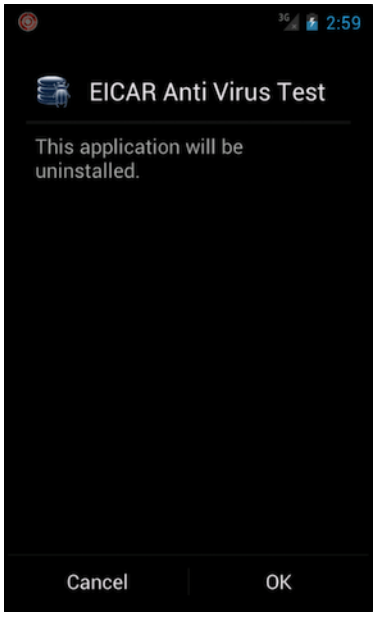
Next, you can view the list of scanned applications on the device. Any malicious apps are indicated by a red warning icon, along with the name of the detection. Any custom detections are indicated by a yellow warning icon and the name of the custom detection list.



Selecting the detected app from the list will display additional information about the app. Select **Uninstall** to remove the malicious or unwanted app.



Select **OK** to proceed with removal of the app. You will then be notified that the app was successfully uninstalled.



CHAPTER 12
ENDPOINT IOC SCANNER

The **Endpoint IOC** (indication of compromise) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers. Endpoint IOCs are imported through the Console from open IOC-based files that are written to trigger on file properties, such as name, size, hash, and other attributes, and system properties, such as process information, running services, and Windows Registry entries.

The IOC syntax can be used by incident responders to find specific artifacts or to use logic to create sophisticated, correlated detections for families of malware. Endpoint IOCs have the advantage of being portable to share within your organization or in industry vertical forums and mailing lists.

The Endpoint IOC scanner is available in AMP for Endpoints Windows Connector versions 4 and higher. Running Endpoint IOC scans may require up to 1 GB of free drive space.

For a listing of IOC attributes that are currently supported by the IOC Scanner and links to sample Endpoint IOC documents see the Cisco Endpoint IOC Attributes guide.

Installed Endpoint IOCs

The **Installed Endpoint IOCs** page lists all the Endpoint IOCs you have uploaded and allows you to manage them. From this page, you can upload new Endpoint IOCs, delete existing ones, activate and deactivate them, or view and edit them. You can also click **View All Changes** to see a filtered view of the Audit Log containing only entries for installed Endpoint IOCs.

Uploading Endpoint IOCs

Endpoint IOCs have to be uploaded to the FireAMP Console before you can initiate scans. When you navigate to the Installed Endpoint IOCs page use the **Upload** button to transfer your

Endpoint IOCs. You can upload a single XML file or a zip archive containing multiple Endpoint IOC documents.

IMPORTANT! There is a 5 MB file upload limit.

If you upload an archive containing multiple Endpoint IOCs you will receive an email when all the files have been extracted and verified. Invalid XML files will be uploaded but cannot be activated for scans.

Each Endpoint IOC entry has a **View Changes** link to take you to the Audit Log with a view filtered to only show entries for that specific Endpoint IOC. This allows you to see who uploaded, edited, activated, deactivated, or otherwise modified the IOC.

View and Edit

The **View** and **Edit** pages allow you to view and modify individual Endpoint IOCs.

The **Short Description** and **Description** are initially pulled from the XML of the Endpoint IOC document. You can change these fields without affecting the IOC itself.

You can assign **Categories**, **Endpoint IOC Groups**, and **Keywords** to each Endpoint IOC to allow you to filter them from the main list. This can be useful if you want to enable or disable all Endpoint IOCs of a certain type. Once you have finished modifying your Endpoint IOC you can Save the changes.

From the Edit page you can **Download** the IOC or **Replace** it. This can be used to edit the indicators and Indicator Items in your Endpoint IOC. Using **Replace** instead of uploading the edited Endpoint IOC will also preserve your assigned Categories, Endpoint IOC Groups, and Keywords.

IMPORTANT! If you upload an Endpoint IOC document with attributes that are not supported by the AMP for Endpoints Connector they will be ignored. For a list of supported IOC attributes see the Cisco Endpoint IOC Attributes guide.

Activate Endpoint IOCs

By default, all new Endpoint IOCs that you upload will be active if they are valid. You can activate or deactivate individual Endpoint IOCs by clicking the **Active** check box next to each one on the Installed Endpoint IOCs page. Click the **Activate All** check box to activate all the Endpoint IOCs in the current view.

You can also use the **Categories, Groups,** and **Keywords** filters to display certain Endpoint IOCs then use **Activate All** to either activate or deactivate them. You can also use the **All**, **Active, Inactive**, **Valid,** and **Invalid** buttons to quickly change your view of the listed IOC documents. This is useful to sort through large sets of Endpoint IOCs and only scan for certain ones.

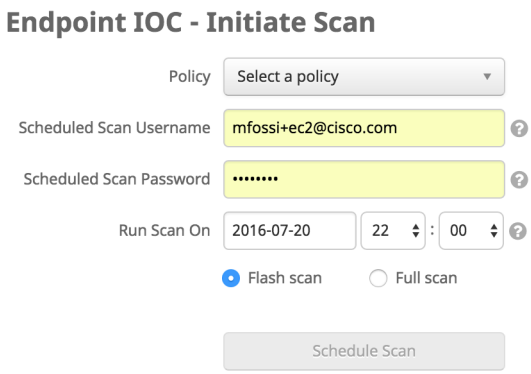
Initiate Scan

You can scan individual computers for matching Endpoint IOCs or all computers in groups that utilize the same policy.

Scan by Policy

To scan by policy, navigate to **Outbreak Control** > **Endpoint IOC - Initiate Scan**. Select the **Policy** you want to add the scan to. Every computer in every group that uses the policy you select will perform the same Endpoint IOC scan.

IMPORTANT! To scan individual computers, see Scan by Computer.



Scheduled Scan Username is the username on the local computer or domain the scan performs as.

Scheduled Scan Password is the password used for the Scheduled Scan Username account.

Run Scan On is the date and time the scan should begin. The time corresponds to the local time on the computer the AMP for Endpoints Connector is running on.

You can select to run a **Flash Scan** or a **Full Scan**. While both scan a similar subset, Full Scan is more comprehensive. As a result, some IOCs may not trigger on Flash Scan if they look for matches in locations that the Flash Scan does not check.

Both **Flash Scan** and **Full Scan** check the following information:

- Running processes
- Loaded DLLs
- Services
- Drivers
- Task Scheduler
- System information
- User account information
- Browser history and downloads

- Windows event logs
- Network and DNS information

Full Scan adds the following:

- The entire Windows registry using the hives on disk
- All files and directories on the file system
- System restore points

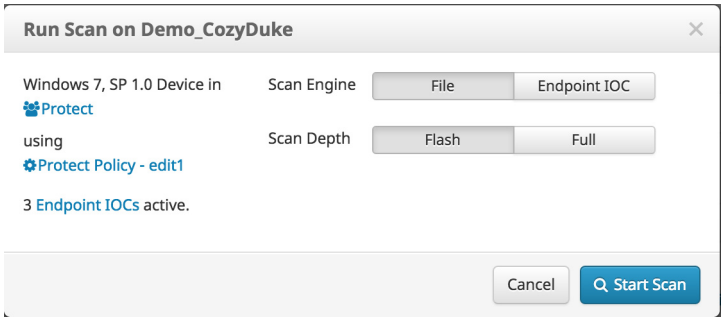
WARNING! Running a full scan is time consuming and resource intensive. On endpoints with a large number of files a full scan can take multiple days to run. You should only schedule full scans during periods of inactivity like at night or on weekends. The first time you run a full scan on a Connector the system will be cataloged, which will take longer than a regular full scan.

If you select a full scan, you can also choose whether to do a full catalog before the scan, catalog only the changes since the last scan (only available on AMP for Endpoints Connector 4.4 and higher), or run the scan without cataloging. A full catalog will take the most time to complete, and running the scan without a catalog will take the least amount of time. If you choose to only catalog changes, then only changes to the filesystem since the last full catalog will be cataloged. The amount of time this scan takes will vary based on the number of changes to catalog.

IMPORTANT! If you have not performed a full catalog on a computer yet and choose not to catalog before the scan then nothing will be scanned.

Scan by Computer

You can also run an Endpoint IOC scan on a single computer by navigating to **Management** > **Computers**. Select the computer you want to scan, then click the **Scan** button.



From the dialog, select the Endpoint IOC scan engine, then choose whether to perform a flash scan or a full scan. As with policy scans, you can also re-catalog the computer when performing a full scan.

When you click **Start Scan,** the AMP for Endpoints Connector will begin the Endpoint IOC scan on its next Heartbeat Interval.

Scan Summary

The **Scan Summary** page lists all the Endpoint IOC scans that have been scheduled in your AMP for Endpoints deployment. Both scheduled scans by policy and scans for individual computers are listed. You can use the **View All Changes** link to see a filtered view of the Audit Log, which shows only Endpoint IOC scans, or click **View Changes** next to a specific scan to see the records only for that specific scan.

For policy scans, the name of the policy is displayed along with the scheduled date and time. For computer scans, the name of the computer is displayed along with the date and time the scan was initiated. You can stop a scan by clicking the **Terminate** button.

IMPORTANT! Terminating a scan is done by sending the Connector a policy update. The Connector will only terminate a scan when it receives the updated policy on its next Heartbeat Interval.

Click the **New Scan** button to schedule another scan by policy. This will take you to the Initiate Scan page.

The results of any Endpoint IOC scans along with matching IOC triggers for each computer scanned will be displayed in the Events Tab of the AMP for Endpoints Dashboard.

CHAPTER 13
SEARCH

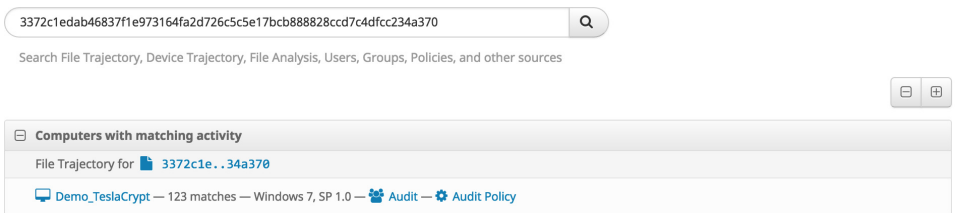
Search allows you to find various information from your AMP for Endpoints deployment. You can search by terms like file, hostname, URL, IP address, device name, user name, policy name and other terms. The searches will return results from **File Trajectory, Device Trajectory, File Analysis** and other sources. To access Search you can navigate through **Analysis > Search** or right-click various elements in the AMP for Endpoints Console like a SHA-256 or file name and select **Search** from the context menu.

TIP! You can also access the search function from the menu bar on any page.

Hash Search

You can enter a file's SHA-256 value to find any devices that observed the file. You can also drag a file to the Search box and its SHA-256 value will be computed for you. If you only have a file's MD5 or SHA-1 value, Search will attempt to match it to a corresponding SHA-256, then search for that SHA-256.

The results can include links to **File Analysis**, **File Trajectory** and the **Device Trajectory** of any AMP for Endpoints Connectors that observed the file.



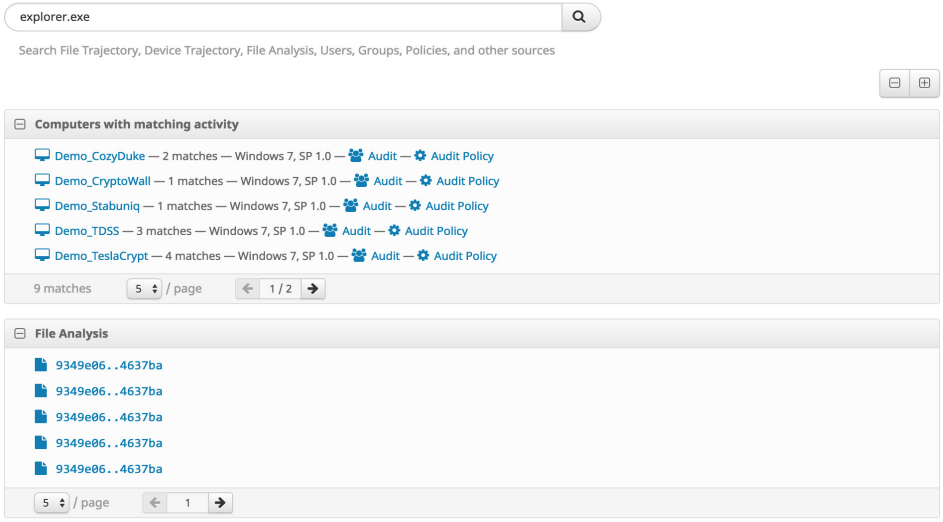
String Search

You can search by entering a string to see matches from various sources. String searches can include:

- file names
- file paths
- detection names
- program names
- program versions
- file versions
- AMP for Endpoints policy names
- AMP for Endpoints group names
- device names (prefix match only)

Searches by exact file extension like `.exe` and `.pdf` can also be performed to find all files observed with those extensions.

Enter an exact email address or user name to find any matching users in your AMP for Endpoints deployment.

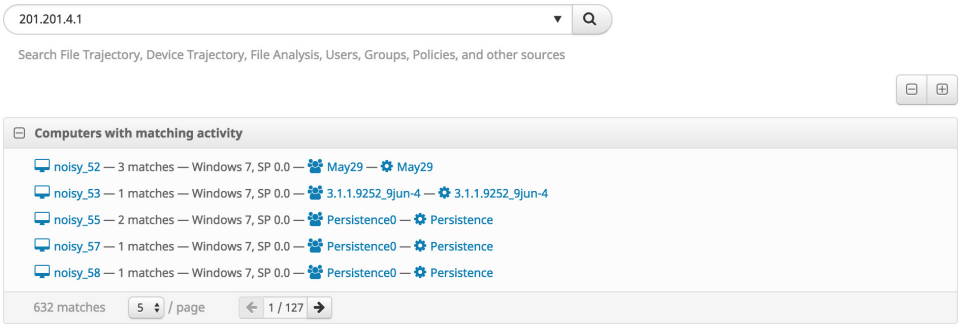


Network Activity Searches

Searches for IP addresses, host names, and URLs can also be performed.

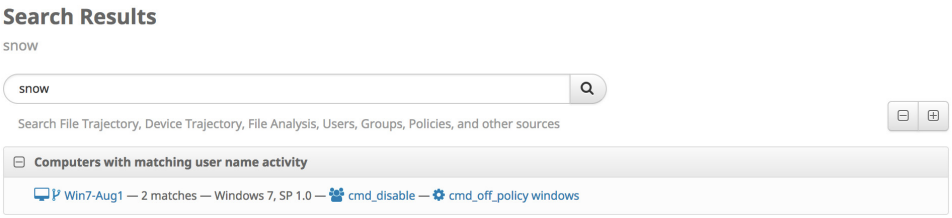
IP address searches must be exact and use the full 32 bits in dot-decimal notation. IP address search results can include devices that have contacted that address or that have observed that IP.

Host name and URL searches can be performed by exact host name or a sub-domain. These searches will return any files that your AMP for Endpoints Connectors downloaded from those hosts and any AMP for Endpoints Connectors that contacted that host.



User Name Searches

You can search by user name to retrieve a list of endpoints with activity initiated by that user. If you search for 'username' then the search will include results for all users in your business with a matching name. However, if you search for 'username@domain' then only endpoints with exact matches will be returned.



You can click on the name of a computer in the search results to view the Device Trajectory for that computer and any events that are associated with the user name.

IMPORTANT! You must have **Send User Name in Events** and **Command Line Capture** enabled in your Policies to be able to search by user name.

CHAPTER 14
FILE ANALYSIS

File Analysis allows an AMP for Endpoints user to upload an executable into a sandbox environment where it is placed in a queue to be executed and analyzed automatically. The File Analysis page also allows you to search for the SHA-256 of an executable to find out if the file has been analyzed already. If the file has been analyzed already, then the analysis report is available and can be viewed by the user. This functionality is provided by Cisco AMP Threat Grid.

To navigate to the File Analysis page click on **Analysis > File Analysis**.

File Analysis Landing Page

When you navigate to File Analysis you will be taken to a listing of files you have submitted for analysis. If you have not submitted any files, you will be taken to the **Global Files** tab, which shows files that AMP Threat Grid users have submitted. From this page you can submit a file for analysis, search for a file by SHA-256 or filename, or view the list of submitted files. When you search for a file, the Global Files tab will show all of your files plus others submitted to Threat Grid; the **Your Files** tab will only show results from your files that were submitted for analysis. Click on the file name or the **Report** button to view the results of the analysis.

IMPORTANT! File Analysis reports are best viewed in Microsoft Internet Explorer 11+, Mozilla Firefox 14+, Apple Safari 6+, or Google Chrome 20+.

If the file you are looking for has not been analyzed already, you can choose to upload the file (up to 20MB) to be analyzed. To do this, click **Submit File**, select the file you want to upload using the **Browse** button, select the virtual machine operating system image to run it in, then

click the **Upload** button. After the file has been uploaded it takes approximately 30 to 60 minutes for the analysis to be available, depending on system load.

IMPORTANT! There are limits to how many files you can submit for analysis per day. By default, you can submit 100 files per day unless you have entered a custom Cisco AMP Threat Grid API key on the Business page. The number of submissions you have available will be displayed on the **Submission** dialog.

If you want to submit a file for analysis that has already been quarantined by your antivirus product, you will need to restore the file before you can submit it. For some antivirus products, there may be specific tools or steps required to restore the file into a usable format since they are often encrypted when quarantined. See your antivirus software vendor's documentation for specific information.

The **File Analysis** sandbox has the following limitations:

- File names are limited to 59 Unicode characters.
- Files may not be smaller than 16 bytes or larger than 20 MB.
- Supported file types are .exe, .dll, .jar, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn, .sep, and .swf.

Once a file has been analyzed you can expand the entry to see the Threat Score and score for the Behavioral Indicators.

Threat Analysis

The analysis of a specific file is broken up into several sections. Some sections may not be available for all file types. You can also download the original sample (executable) that was executed in the sandbox. This is useful if you want to perform a deep analysis on the executable and it can also be used to create Custom Detections - Simple and Custom Detections - Advanced lists to control and remove outbreaks in a network.

WARNING! Files downloaded from the File Analysis are often live malware and should be treated with extreme caution.

When analyzing malware, a video of the execution is also captured. The video can be used to observe the visual impact that the malware has on the desktop of a victim. The video can be used in user education campaigns; for example, in the case of an outbreak, the security analyst can send screenshots of behavior of this threat to network users and warn them of symptoms. It can also be used to warn about convincing social engineering attacks like phishing; for example, the fake antivirus alerts common with malicious fake antivirus or scareware.

You can also download the entire network capture that was collected while analyzing the binary by clicking on **Download PCAP**. This network capture is in PCAP format and can be opened with network traffic analysis tools such as Wireshark. The availability of this network

capture file means that a security analyst can create a robust IDS signature to detect or block activity that is associated with this threat.

If the malware creates any other files during execution, they will be listed under **Artifacts**. You can download each artifact and run a separate analysis on them.

Metadata

Basic information pertaining to the analysis is displayed at the top of the **Analysis Report**. This includes basic characteristics of the submission, as shown below.

ID: A unique identifier that is assigned to each sample when it is submitted for analysis.

OS: The operating system image used when the sample was analyzed.

Started: The date and time when the analysis started.

Ended: The date and time when the analysis ended.

Duration: The amount of time it took for the analysis to complete.

Sandbox: Identifies the sandbox used during the analysis.

Filename: The name of the sample file that was submitted for analysis, or the file name that was entered when a URL sample was submitted.

Magic Type: This field indicates the actual file type detected by the AMP Threat Grid analysis.

Analyzed As: Indicates whether the sample was analyzed as a URL or as a file (by specifying the file type).

SHA256: The SHA-256 cryptographic hash function output.

SHA1: The SHA1 cryptographic hash function output.

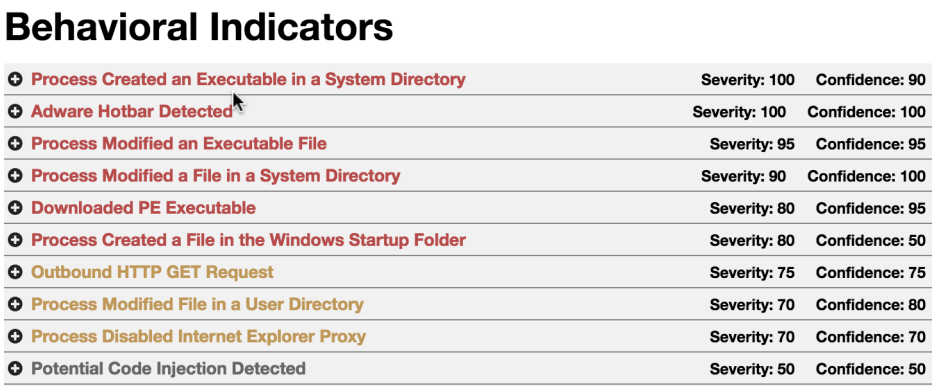
MD5: The MD5 cryptographic hash function output.

Warnings: High level descriptions of potentially harmful activities.

Behavioral Indicators

The analysis report provides a summary of the behavioral indicators generated by AMP Threat Grid analysis. These indicators quickly explain any behaviors that might indicate malicious or

suspicious activity. AMP Threat Grid generates behavioral indicators during analysis, after the analysis of the malware activities is complete.



Behavior indicators include detailed descriptions of the activity that produced the indicator. They also include information on why malware authors leverage that specific technique, plus the specific content that caused the indicator to trigger during analysis.

Threat Score

The top row of the **Behavioral Indicators** section of the Analysis Report includes an overall threat score that can be used as a general indicator of the likelihood that the submission is malicious.

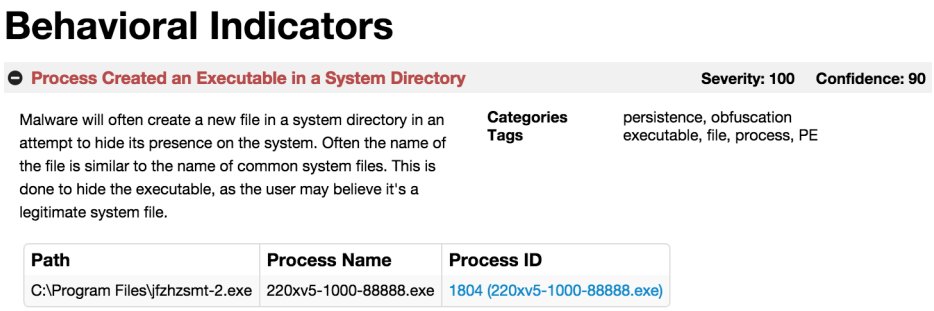
The algorithm used to calculate the threat score is based on a variety of factors, including the number and type of behavioral indicators, in conjunction with their individual confidence and severity scores.

Behavioral indicators are listed in order by priority according to their potential severity (with most severe threats listed first), which is reflected by the color coding:

- Red: This is a strong indicator of a malicious activity.
- Orange: This is a suspicious activity and the analyst should carefully assess the submission.
- Grey: Indicates that these activities are not normally leveraged by malicious software, but provide some additional indicators that could help the analyst come to their own conclusion.

Behavioral Indicator Detail

Additional detailed information can be viewed by clicking on the + beside each behavioral indicator. Detailed information will vary according to the behavioral indicator type. The display will present information that is relevant and applicable to each particular type of alert.



Description: A description of why the behavior is suspicious.

Categories: Shows whether a particular behavioral indicator is associated with a family of threats or malware. This information is helpful when you're searching for related malware.

Tags: These are tags that are assigned automatically by behavioral indicators to help summarize characteristics and activities.

The following fields will be included depending on the type of sample that was analyzed.

Address: The process address space.

Antivirus Product: The name of the antivirus product that flagged the sample as potentially malicious.

Antivirus Result: Shows the results of the flagged antivirus product.

Artifact ID: The ID of any artifacts generated by the sample. The link on the ID takes the user to the section of the Analysis Report for that artifact.

Callback Address: The callback verification address used by the behavioral indicator.

Callback RVA: The callback's relative virtual address.

Flags - List of flags generated by the behavioral indicator.

md5 - The MD5 checksum of the file.

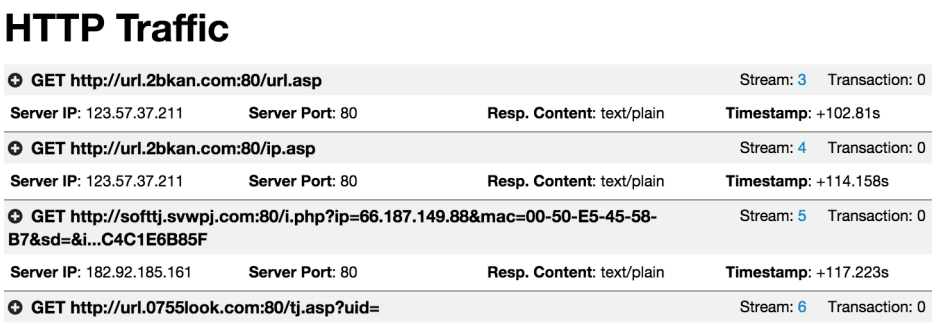
Path - The full path of any files created or modified during execution.

Process ID - The process ID of any processes created during execution.

Process Name - The name of any processes created during execution.

HTTP Traffic

If AMP Threat Grid detects HTTP traffic during sample analysis, the activity will be displayed, showing the details of each HTTP request and response, such as the HTTP command used.



DNS Traffic

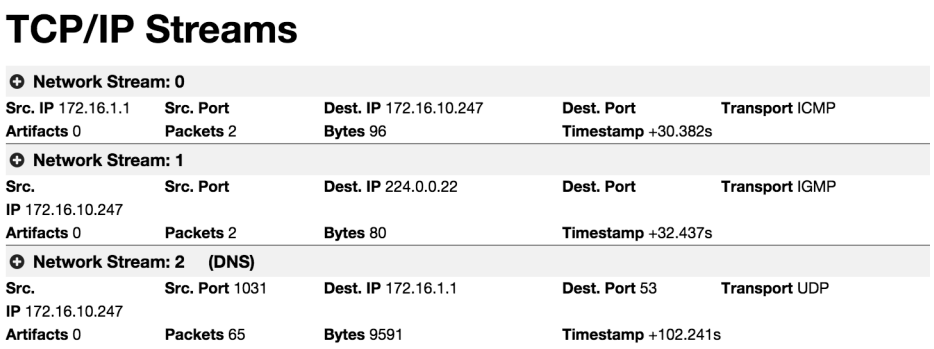
If AMP Threat Grid detects any DNS queries for IP addresses of external host names during analysis, the results will be displayed in this section.

TCP/IP Streams

The **TCP/IP Streams** section of the Analysis Report displays all of the network sessions launched by the submission.

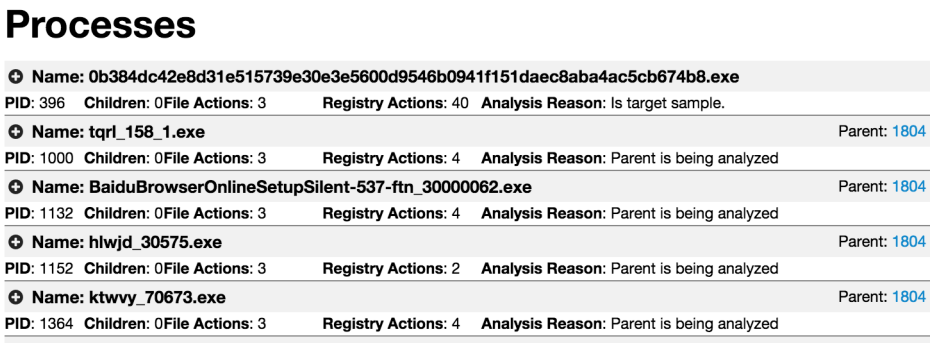
Move the cursor over the Src. IP address to display a pop-up listing all the source network IP addresses of the network stream that have been detected by AMP Threat Grid during analysis.

Clicking on one of the network streams will open a web page with the appropriate network stream.



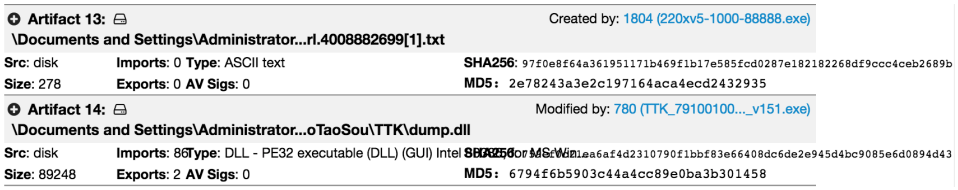
Processes

If any processes are launched during the submission analysis, AMP Threat Grid displays them in this section. Click the + icon next to a process to expand the section and access more detailed information.



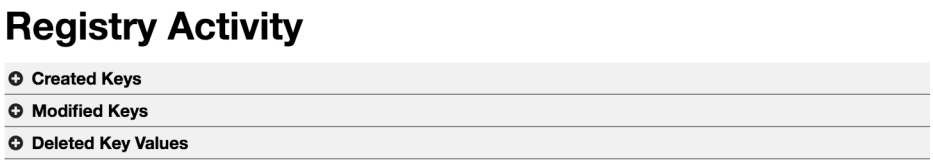
Artifacts

If any artifacts (files) are created during the submission analysis, AMP Threat Grid displays summary information for each artifact. Click the + icon next to an artifact to expand the section and access more detailed information.



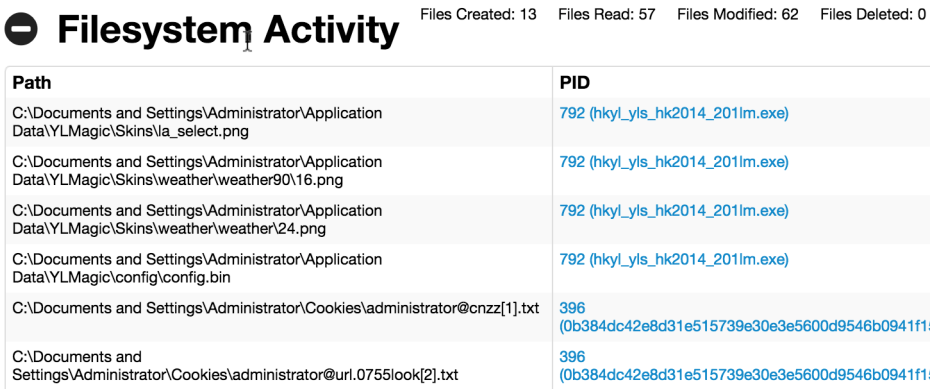
Registry Activity

If analysis detects changes to the registry, AMP Threat Grid displays them in this section. Click the + icon next to a registry activity record to expand the section and access more detailed information.



Filesystem Activity

If any filesystem activity (file creation, modification, or reads) is detected during the submission analysis, AMP Threat Grid presents a summary of the activity information. Click the + icon next to a filesystem record to expand the section and access more detailed information.



CHAPTER 15
TRAJECTORY

Trajectory shows you activity within your AMP for Endpoints deployment, either across multiple computers or on a single computer.

File Trajectory

File Trajectory shows the life cycle of each file in your environment from the first time it was seen to the last time, as well as all computers in the network that had it. Where applicable, the parent that brought the threat into the network is displayed, including any files created or executed by the threat. Actions performed throughout the trajectory for a file are still shown even if the antivirus software on the computer was later disabled.

Description

File trajectory is capable of storing approximately the 9 million most recent file events recorded in your environment. When a file triggers an event, the file is cached for a period of time before it will trigger another event. The cache time is dependent on the disposition of the file:

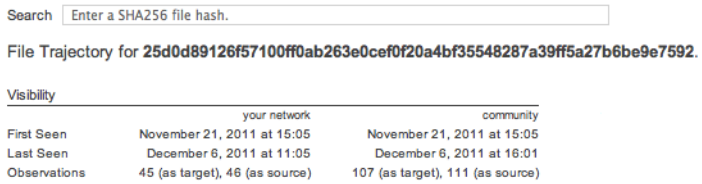
- Clean files: 7 days
- Unknown files: 1 hour
- Malicious files: 1 hour

File Trajectory displays the following file types:

- Executable files
- Portable Document Format (PDF) files
- MS Cabinet files
- MS Office files

- Archive files
- Adobe Shockwave Flash
- Plain text files
- Rich text files
- Script files
- Installer files

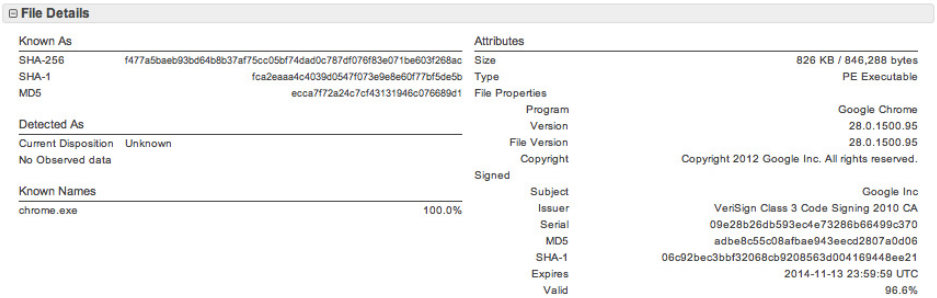
Visibility includes the **First Seen** and **Last Seen** dates and the total number of observations of the file in question in your network. **Observations** shows the number of times that the file in question was both a source of activity and when it was a target of activity. Note that the number of observations can also include multiple instances of the same file on each endpoint.



Entry Point – identifies the first computer in your network on which the threat was observed.

Created By identifies the files that created the threat in question by their SHA-256. This includes the number of times the threat was created by that file in both your network and among all AMP for Endpoints users. Where available the file name and product information are also included. It is important to note that this information is pulled from the file itself. In some cases a malicious (red) file can include information claiming it is a legitimate file.

File Details shows additional information about the file in question, as outlined below.

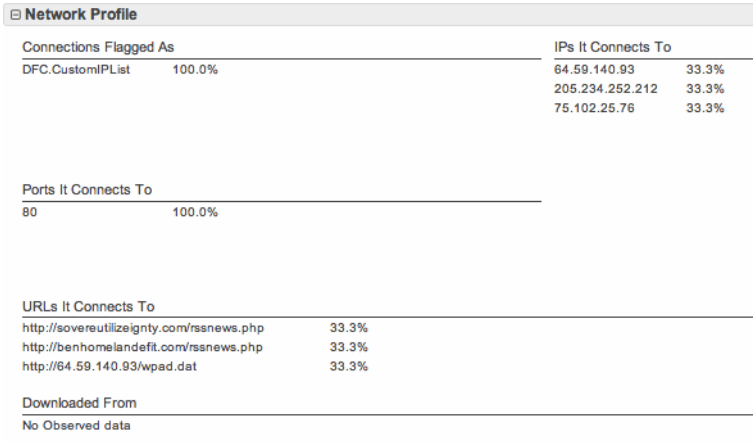


- **Known As** shows the SHA-256, SHA-1, and MD5 hash of the file.
- **Attributes** displays the file size and type.

- **Known Names** includes any names the file went by on your network.
- **Detected As** shows any detection names in the case of a malicious file.

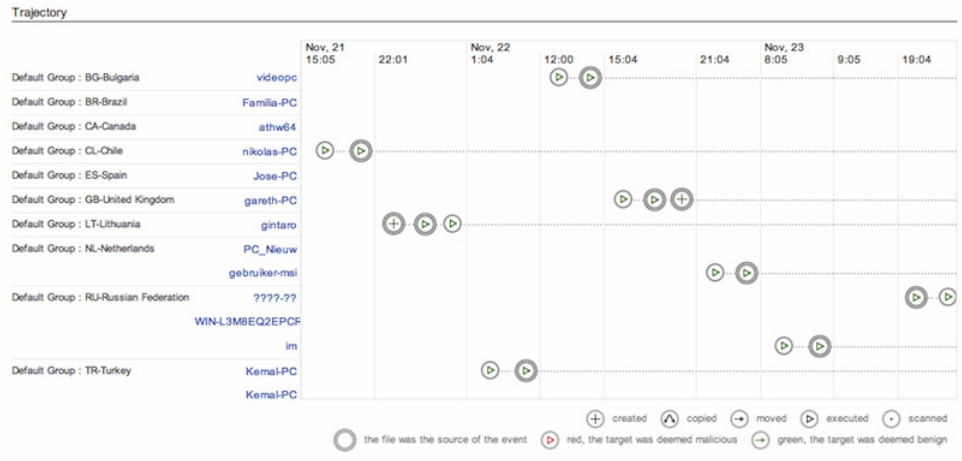
> **IMPORTANT!** For descriptions of threat names, see AMP Naming Conventions.

Network Profile shows any network activity the file may have participated in. If there are no entries in this section, this does not necessarily mean the file is not capable of it, but your Connectors did not observe it participating in any while it was in your environment. If your Connectors do not have Device Flow Correlation enabled, this section will not be populated. Network Profile details are as shown below.



- **Connections Flagged As** shows any activity that corresponds to an **IP blacklist** entry.
- **IPs it Connects To** lists any IP addresses the file initiated a connection to.
- **Ports it Connects To** lists the ports associated with outbound connections from the file.
- **URLs it Connects To** lists any URLs that the file initiated a connection to.
- **Downloaded From** lists any addresses that the file in question was downloaded from.

Trajectory – shows the date and time of each action related to the threat on each affected computer in your environment.



Actions tracked are shown in the box below.

	A benign file copied itself
	A detected file copied itself
	A file of unknown disposition copied itself
	A benign file was created
	A detected file was created
	A file of unknown disposition was created
	A benign file was executed
	A detected file was executed
	A file of unknown disposition was executed
	A benign file was moved
	A detected file was moved
	A file of unknown disposition was moved
	A benign file was scanned
	A detected file was scanned
	A file of unknown disposition was scanned

	A file was successfully convicted by TETRA or ClamAV
	A benign file was opened
	A detected file was opened
	A file of unknown disposition was opened

When an action has a double circle around it  , this means the file in question was the source of the activity. When there is only a single circle, this means that the file was being acted upon by another file.

Clicking on a computer name will provide more detail on the parent and target actions and SHA-256s for the file being examined.

By clicking on one of the action icons in the **Trajectory** display, you can also view additional details including the filename and path if available.

Event History shows a detailed list of each event identified in the Trajectory. Events are listed chronologically by default but can be sorted by any of the columns.

Device Trajectory

Device Trajectory shows activity on specific computers that have deployed the AMP for Endpoints Connector. It tracks file, network, and Connector events, such as policy updates in chronological order. This gives you visibility into the events that occurred leading up to and following a compromise, including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware.

Description

Device Trajectory is capable of storing approximately the 9 million most recent file events - approximately 31 days for a typical AMP for Endpoints business - recorded in your environment. When a file triggers an event the file is cached for a period of time before it will trigger another event. The cache time is dependent on the disposition of the file:

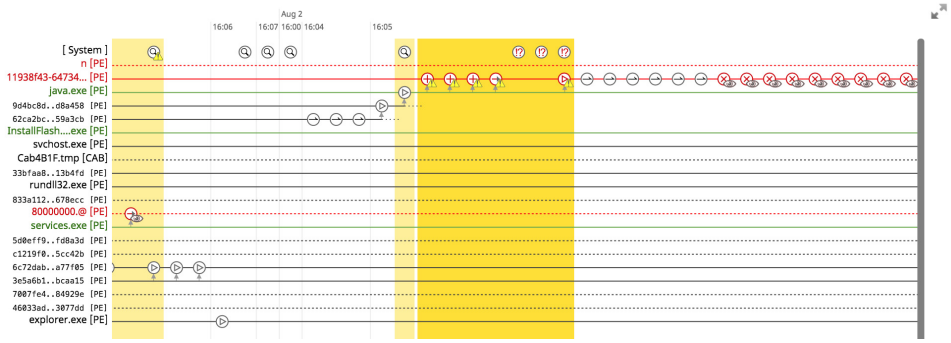
- Clean files – 7 days
- Unknown files – 1 hour
- Malicious files – 1 hour

Device Trajectory displays the following file types:

- Executable files
- Portable Document Format (PDF) files
- MS Cabinet files
- MS Office files
- Archive files
- Adobe Shockwave Flash
- Plain text files
- Rich text files
- Script files
- Installer files

IMPORTANT! A maximum of 4000 objects can be rendered in the Device Trajectory view. If you navigate to Device Trajectory from the **Computers** page, you will see the 4000 most recent objects. If you navigate to Device Trajectory from a specific event, you will see up to 4000 objects related to that event.

The vertical axis of the Device Trajectory shows a list of files and processes observed on the computer by the AMP for Endpoints Connector and the horizontal axis represents the time and date. Running processes are represented by a solid horizontal line with child processes and files the process acted upon stemming from the line. Click on an event to view its details.



File events include the file name, path, parent process, file size, execution context, and hashes for the file. For malicious files, the detection name, engine that detected the file, and the quarantine action are also shown.

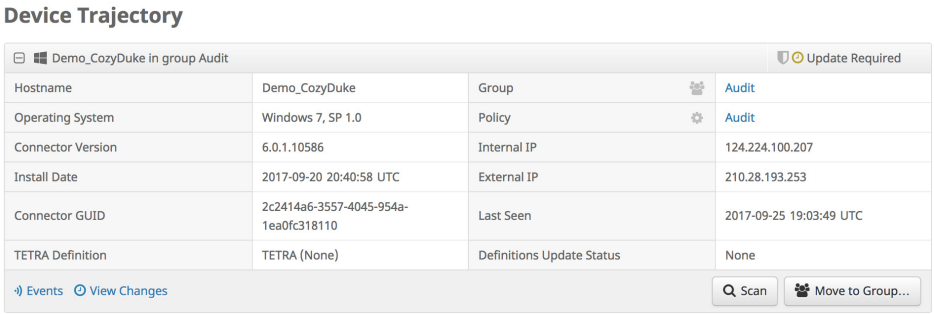
IMPORTANT! For descriptions of threat names, see AMP Naming Conventions.

Network events include the process attempting the connection, destination IP address, source and destination ports, protocol, execution context, file size and age, the process ID and SID, and the file's hashes. For connections to malicious sites, the detection name and action taken will also be displayed.

AMP for Endpoints Connector events are displayed next to the [System] label in Device Trajectory. Connector events include reboots, user-initiated scans and scheduled scans, policy and definition updates, Connector updates, and a Connector uninstall.

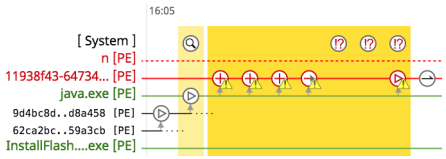
You can use the slider below the device trajectory to narrow the scope of the trajectory to a specific time and date range. The left handle of the slider changes the beginning of the trajectory view and the right handle limits the end of the view. This can help you see the trajectory of events in a particular time range with greater clarity.

You can view details of the selected computer from the Device Trajectory view by clicking on the computer name in the Device Trajectory view.



Indications of Compromise

When certain series of events are observed on a single computer, they are seen by AMP for Endpoints as indications of compromise. In Device Trajectory, these events will be highlighted yellow so they are readily visible. There will also be a separate compromised event in the Trajectory that describes the type of compromise. Clicking on the compromised event will also highlight the individual events that triggered it with a blue halo.



For indication of compromise descriptions, please see Threat Descriptions.

Filters and Search

Device Trajectory can contain a large amount of data for computers that see heavy use. To narrow Device Trajectory results for a computer, you can apply filters to the data or search for specific files, IP addresses, or threats. You can also use filters in combination with a search to obtain even more granular results.

Filters

There are four event filter categories in Device Trajectory: **Event Type**, **Event Disposition**, **Event Flags**, and **File Type**. You must select at least one item from each category to view results.

Event Type describes events that the AMP for Endpoints Connector recorded. File, network, and Connector activity are represented.

File events can include a copy, move, execution, and other operations. Network events include both inbound and outbound connections to both local and remote addresses. Connector activity can include reboots, policy updates, scans, and uninstalls.

Event Disposition allows you to filter events based on their disposition. You can choose to view only events that were performed on or by malicious files, clean files, or those with an unknown disposition.

Event Flags are modifiers to event types. For example, a warning may be attached to a malicious file copy event because the malicious file was detected but not successfully quarantined. Other events, such as a scan that did not complete successfully or a failed policy update, may also have a warning flag attached.

The **audit only** flag means that the events in question were observed but not acted upon in any way because the **File Conviction Mode** policy item under File > Modes or the **Detection Action** policy item under Network > Device Flow Correlation (DFC) was set to **Audit**.

File Type allows you to filter Device Trajectory events by the type of files involved.You can filter by the file types most commonly implicated in malware infections, such as executables and PDFs. The **other** filter is for all file types not specifically listed, while the **unknown** filter is for files that the type was undetermined, possibly due to malformed header information.

Search

The search field on the Device Trajectory page allows you to narrow the Device Trajectory to only show specific results. Searches can be simple text strings, a regular expression supported by JavaScript in the `/foo/gim` format where the `gim` are optional flags, or a CIDR address in the format `X.X.X.X/Y`. You can also drag and drop a file into the search box on browsers that support this, which will calculate the SHA-256 value of the file and insert the string in the search box.

Within Device Trajectory events, there are several terms you can search by including:

- Detection name
- SHA-256
- SHA-1
- MD5
- File name

- Directory name
- Local and remote IP addresses
- Port numbers
- URLs

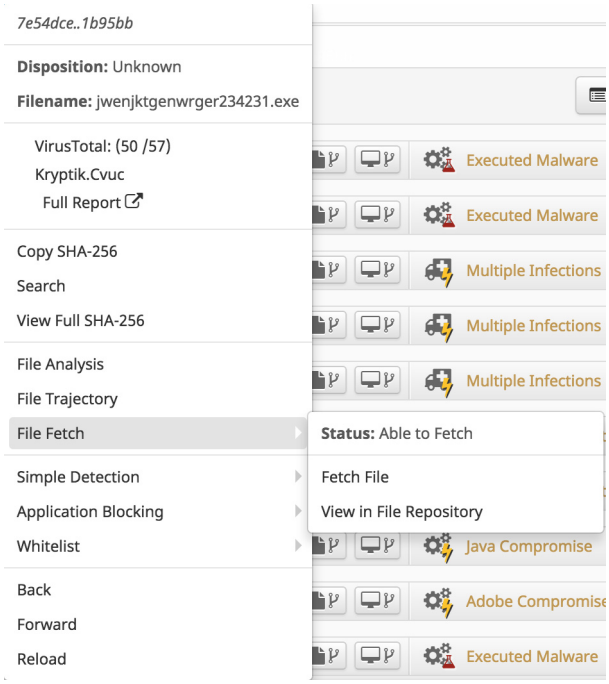
CHAPTER 16
FILE REPOSITORY

The **File Repository** allows you to download files you have requested from your AMP for Endpoints Connectors. This feature is useful for performing analysis on suspicious and malicious files observed by your Connectors. You can simply request the file from any of the Connectors that observed it, wait for the file to be uploaded, then download it to a virtual machine for analysis. You can also submit the file to File Analysis for additional decision support. Clicking **View All Changes** will take you to a filtered view of the Audit Log showing all requested files.

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 3.1.9 or later of the AMP for Endpoints Windows Connector, version 1.0.2.6 or later of the AMP for Endpoints Mac Connector, and version 1.0.2.261 or later of the AMP for Endpoints Linux Connector.

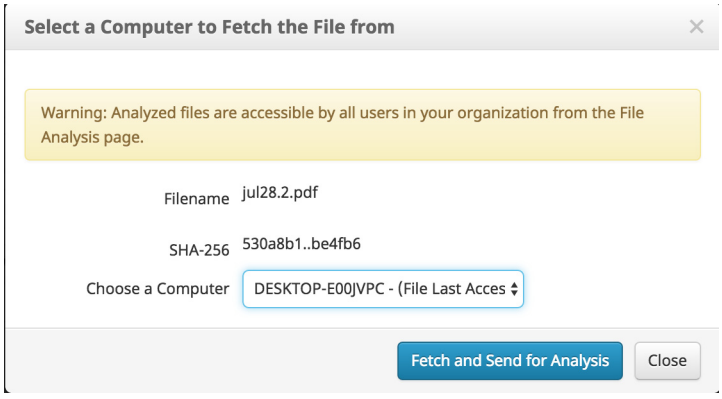
Requesting a remote file

To request a file for upload to the File Repository, right-click on any SHA-256 value in the AMP for Endpoints Console to bring up the SHA-256 File Info Context Menu.



Select **Fetch File** from the menu. If the file has already been downloaded to the File Repository, Fetch File will not be available and instead there will be an option to view the file in the repository.

A dialog will appear allowing you to select which AMP for Endpoints Connector to download the file from. If the file was observed by more than one Connector, you can use the drop-down list to select a specific computer out of up to ten computers that saw the file recently. The default selection is the Connector that observed the file most recently.

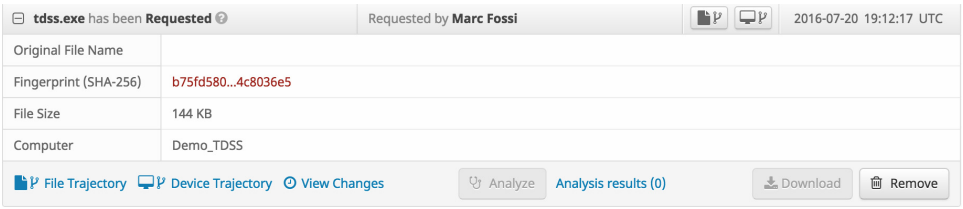


Once you have selected a computer, click **Fetch** to be taken to the File Repository. There you will see an entry for the file and that it has been requested. Files in the Repository can be in the following states:

- Requested: a request was made to upload the file but the Connector has not responded yet.
- Being Processed: the file has been uploaded from the Connector but is still being processed before it is available.
- Available: the file is available for download.
- Failed: an error occurred while the file was being processed.

IMPORTANT! If an upload fails after multiple attempts to fetch it contact Support.

You will receive an email notification when the file has been processed. Navigate to the File Repository page to download the file. You can also launch the Device Trajectory for the computer the file was retrieved from or launch the File Trajectory. Clicking **Remove** will delete the file from the Repository but not from the computer it was fetched from. You can also click **View Changes** to see the Audit Log entry for the request.



When you download a file from the File Repository it will be a password-protected zip archive containing the original file. The password for the archive will be “infected”.

WARNING! In some cases you may be downloading live malware from the File Repository. You should only extract the file from the archive in a secure lab environment.

Under certain circumstances a file may not be available for download even though the AMP for Endpoints Connector observed it. This can occur if the file was deleted from the computer or 3rd party antivirus software quarantined the file. Files with a clean disposition cannot be retrieved unless they were copied to a different location. In these cases you can attempt to fetch the file from a different computer or manually retrieve the file from quarantine.

CHAPTER 17
THREAT ROOT CAUSE

Threat Root Cause helps identify legitimate and rogue applications that are at high risk for introducing malware into your environment. It focuses on software that is observed installing malware onto computers.

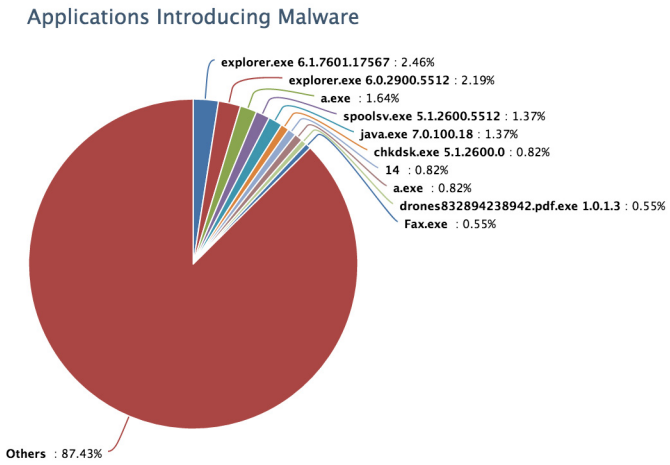
Select Dates

Threat Root Cause allows you to select a date range to view. By default, the date range is set to show the previous day and current day. Select the start and end dates you want to view, then click **Reload** to view the threat root cause for the specified date range.

Overview

The **Threat Root Cause Overview** tab shows the top ten software packages by name that have been observed introducing malware into your environment in the past day. The “Others” entry

is an aggregate of all other applications introducing malware for comparison purposes. Where available, the version numbers of the applications are also displayed.



Details

The **Details** tab displays each application from the Overview with additional information. The number of threats the application introduced into your environment, the number of computers that were affected, and the event type are also displayed. The information icon can be clicked to display a context menu.

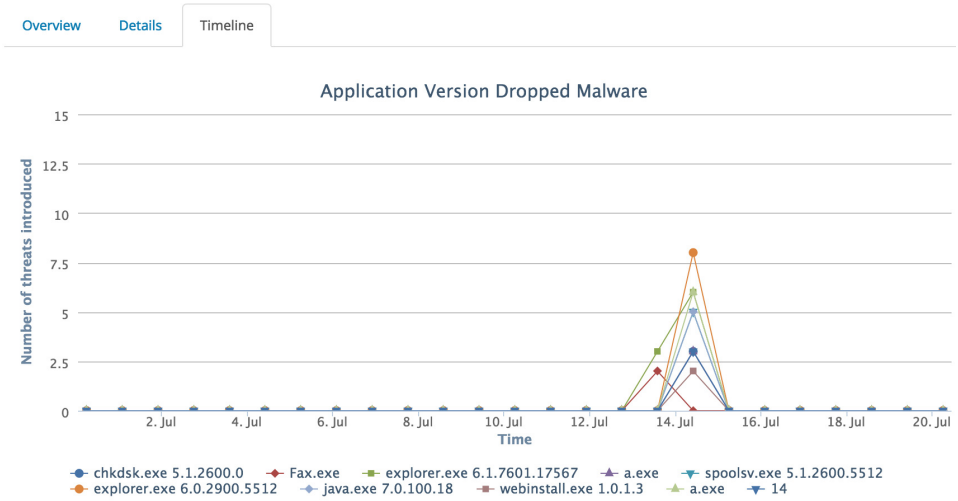
Program	Threat Name	Version	Threats Introduced	Computers Affected	Event Type
explorer.exe		6.1.7601.17567	9	3	6 created 3 executed
explorer.exe		6.0.2900.5512	8	4	4 executed 4 moved
a.exe			6	1	2 created 2 executed 2 moved
spoolsv.exe		5.1.2600.5512	5	1	3 created 2 executed
java.exe		7.0.100.18	5	1	3 created 1 executed 1 moved
a.exe	W32.SPERO.Spero...		3	1	2 created 1 executed
chkdsk.exe		5.1.2600.0	3	1	2 created 1 executed

Clicking on the program name in this view will take you to the Dashboard Events Tab with the view filtered to show all events where the particular program was the parent.

Timeline

The **Timeline** tab shows the frequency of malware downloaded into your environment by each application over the previous day. If one application is seen introducing many malware

samples at once or consistently over the period it can indicate that the application is nothing more than a downloader for malware. There is also a possibility that a vulnerable application being exploited to install malware could display similar behavior.



CHAPTER 18
PREVALENCE

Prevalence displays files that have been executed across your organization in relation to global executions of those files. This can help you surface previously undetected threats that were only seen by a small number of users. Generally, files executed by a large number of users tend to be legitimate applications, while those executed by only one or two users may be malicious, such as a targeted advanced persistent threat.

Low Prevalence Executables

The page shows each file that was executed and which computer it was executed on. The list is filtered by operating system, so that low prevalence files from widely deployed operating systems aren't obscured by those with lower deployment numbers. File disposition is indicated by the color of the filename that was executed with malicious files shown in red and unknown files shown in gray. Files with a known clean disposition are not displayed in the prevalence list.

Expanding an entry shows you the SHA-256 value of the file, the names of up to 10 computers that were seen executing the file, and other filenames the file may have had when executed. You can click the information icon next to the SHA-256 value to display the SHA-256 File Info Context Menu. Click on the **File Trajectory** button to launch the File Trajectory for the file or the Device Trajectory button to view the trajectory for the computer that executed the file. You can also send the file for analysis by clicking the **Analyze** button if you have the File

Repository enabled and the file is a Windows executable. If more than one computer executed the file, click on the name of the computer to view its Device Trajectory.

IMPORTANT! If the **Analyze** button is not available it may be that the file has already been submitted, the **File Repository** is not enabled, or the current user is not an administrator.

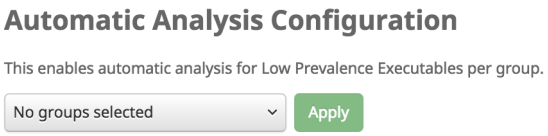
When you click the Analyze button, a request is submitted to retrieve the file from the computer. You can check the status of the file fetch operation from the File Repository. Once the file has been retrieved it will be submitted to File Analysis.

Automatic Analysis

Automatic analysis sends low prevalence Windows executable files from specific groups to File Analysis. Click **Configure Automatic Analysis** to choose your groups.

IMPORTANT! You must have the File Repository enabled and be an administrator before you can configure automatic analysis.

On the **Automatic Analysis Configuration** page there is a drop-down to select the groups you want to automatically submit low prevalence files. Select your groups then click **Apply**.



Once you have configured **Automatic Analysis**, low prevalence executable files will be submitted every 4 hours. AMP for Endpoints will request the file from the AMP for Endpoints Connector that observed it if it is available. Once the file has been retrieved, it will be submitted to **File Analysis**. You can then view the results of the analysis from the File Analysis page. If the file is not retrieved for a period of time, you can check the file fetch status in the File Repository.

IMPORTANT! There are limits to how many files you can submit for analysis per day and their size. By default, you can submit 100 files per day unless you have entered a custom Cisco AMP Threat Grid API key on the Business page and they can be up to 20MB each in size.

CHAPTER 19
VULNERABLE SOFTWARE

Whenever an executable file is moved, copied, or executed the AMP for Endpoints Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the 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.

Currently the following applications and versions on Windows operating systems are reported on the vulnerabilities page:

- Adobe Acrobat 11 and higher
- Adobe Acrobat Reader 9 and higher
- Adobe Flash Player 11 and higher
- Google Chrome 25 and higher
- Microsoft Internet Explorer 8 and higher
- Microsoft Office 2007 and higher
- Mozilla Firefox 10 and higher
- Oracle Java Platform SE 1.7.0 and higher

By default, all known vulnerable programs are shown. The list can be filtered to show only the vulnerable programs detected that day or that week. You can also download the list of vulnerable programs in a CSV file to work with offline.

IMPORTANT! All dates and times in the exported CSV file will be in UTC regardless of your Time Zone Settings.

Each list item can be expanded or collapsed by clicking anywhere on the list. Also, all list items can be expanded or collapsed at the same time by clicking on the (+) or (-) sign.

The list item contains a summary of information on the vulnerability, including:

- Program name and version.
- SHA-256 value for the executable file.
- The number of computers in the defined group that the AMP for Endpoints Connector observed the file on.
- The number of severe vulnerabilities known to be present in the executable. See Common Vulnerabilities and Exposures.
- CVSS score of the most severe vulnerability in the executable. See Common Vulnerability Scoring System.

Common Vulnerabilities and Exposures

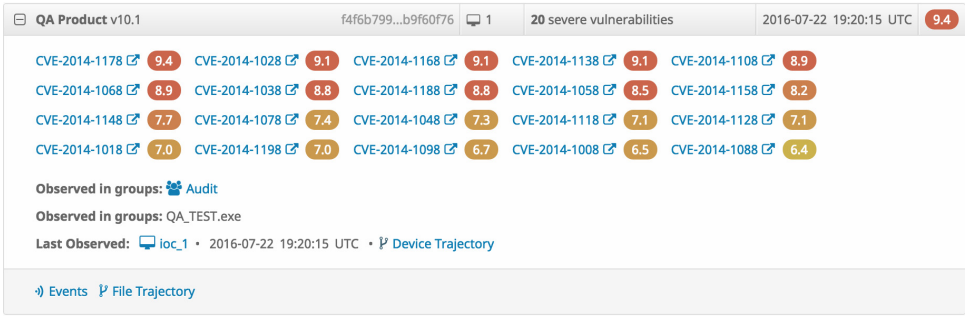
The Common Vulnerabilities and Exposures (CVE) database records known vulnerabilities in various applications. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the Console can be clicked to get more details on the vulnerability.

Clicking on the CVE ID link brings you to a page that defines the vulnerability and lists any patches if available.

Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is designed to allow a user to determine which priority level to assign to an identified vulnerability. The scale goes from 0 (lowest) to 10 (highest).

Clicking on an item in the list of identified vulnerable programs shows the ten most severe and recent vulnerabilities with a CVSS score higher than 5.9.

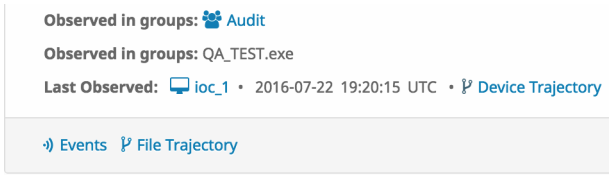


Additional Information on Vulnerable Software

Additional information is available at the bottom of the expanded program list item. The following topics provide additional information through the associated links:

- **Observed in Groups**
- **Last Observed** (computer)
- **Events**
- **File Trajectory**

Additionally, the **Filename** indicates the file name of the executable file.



Observed in Groups

The link (for example, Audit) is the name of the defined group that the computers belong to. For more information see Groups.

Last Observed

The time and date and on which computer the vulnerability was last observed. The machine name is a link to a page which provides additional details on the computer. For more information see Computer Management.

Events

Clicking on the **Events** link opens the **Dashboard** and shows the contents of the **Events** tab. For more information, see Events Tab.

File Trajectory

Clicking on the **File Trajectory** link opens a page showing file trajectory details. For more information, see File Trajectory.

Device Trajectory

Clicking on the **Launch Device Trajectory** link opens a page showing device trajectory details. For more information, see Device Trajectory.

CHAPTER 20
REPORTS

Reports allow you to view aggregate data generated in your business over a one week period. They can be accessed from **Analysis > Reports** on the main menu.

Creating a Report

Reports cover a one week period beginning every Sunday at midnight until midnight the following Sunday (UTC). Weekly reports are created automatically but you can choose whether to receive the reports via email.

Report Sections

Each report section links to the appropriate section of the AMP for Endpoints Console, so you can drill down further into the data.

IMPORTANT! The data displayed in the Console may not match the report data exactly if any retrospective jobs were run after the report was generated.

Active Connectors

Shows the number of active Connectors in the business compared to the previous week. To be considered active, a Connector must have checked in at least once in the 7 day period. The number of new installs and uninstalls are also shown.

Infected Computers Comparison

Shows the number of computers that observed both file-based and network-based detections this week compared to the previous week. The top five computers observing malware are also listed along with the number of malicious file and network detections each saw.

File Detections

Shows the top five computers seeing file detections over the week and the top five files detected. You can also see the daily detection rates for the current week compared to the previous week.

Network Detections

Shows the top five computers seeing network detections over the week and the top five IP addresses detected. You can also see the daily detection rates for the current week compared to the previous week.

Quarantines

Shows the daily successful quarantine rate for the current week compared to the previous week.

Application Blocks

Shows successful application blocks for the week based on your Application Control - Blocking lists.

Retrospective Detections

Shows the number of files seen by your Connectors that had their disposition changed to malicious and were retroactively quarantined.

Retrospective False Positives

Shows the number of files seen by your Connectors that were initially categorized as malicious that had their disposition changed to clean and were retroactively restored from quarantine.

Indications of Compromise

Shows the number of times Indications of Compromise were triggered for the week.

CHAPTER 21
AGENTLESS COGNITIVE INCIDENTS

Agentless incidents are events recorded by Cognitive Threat Analytics (CTA) for your organization. This records incidents that occur on computers that don't have an AMP for Endpoints Connector installed. You must have **Cognitive Threat Analytics Integration** enabled on the Business page and at least one CTA-enabled device like a Cisco Web Security Appliance configured to send logs to CTA for events to populate this page.

Each row has a username (if it can be determined), IP address, and list of cognitive incidents that were detected by your CTA-enabled devices.

Click on a username or IP address to see more information about the incidents observed around the computer. Click on one of the cognitive incident names to learn more about the threat, including all webflows associated with it. Click on a campaign name (noted by the hashtag at the beginning of the name) to view all computers in your organization that observed cognitive incidents related to that specific campaign. A campaign is typically a set of threats that work together, such as a Trojan that in turn downloads a bot.

You should Download and install an AMP for Endpoints Connector on any computers that appear in the **Agentless Cognitive Incidents** list if possible. This can help to detect and quarantine threats at an earlier stage and surface the full range of an incident through Device Trajectory.

CHAPTER 22
ACCOUNTS

Items under the **Accounts** menu allow you to manage your AMP for Endpoints Console. User management, defaults, and audit logs can all be accessed from this menu.

Users

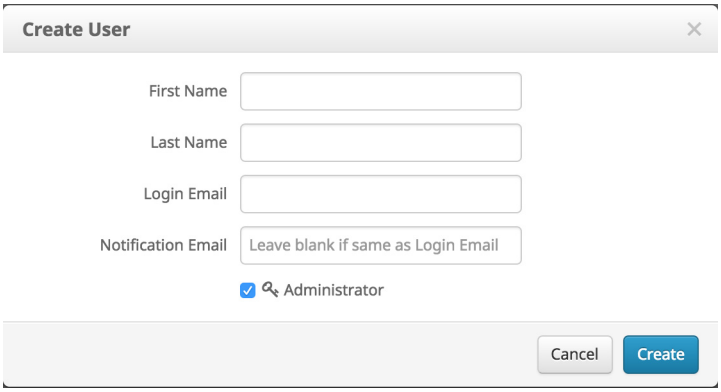
The **Users** screen allows you to manage accounts and view notifications and subscriptions for that account.

You can search the user list by name or email address. You can also sort the list by email address, name, or last login time. Accounts with a key next to them are administrators and those without are unprivileged users. Click the **My Account** link to view the account you are currently logged in as. This account will also be highlighted blue in the user list.

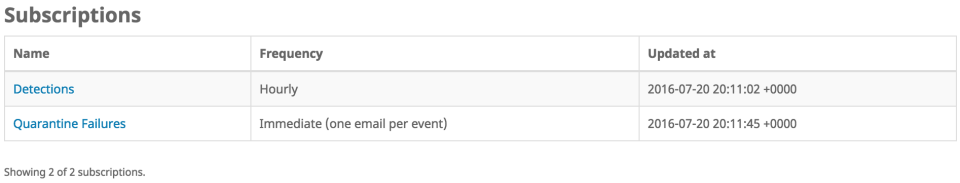
Clicking the clock icon next to a user account will allow you to see a filtered view of the Audit Log for activity related to that account. You can also click the **View All Changes** link to see a filtered view of the Audit Log showing all activity for user accounts.

When you select an account by clicking on **Name** or **Email Address**, you can see different options for it including options to edit the account. If you select your own account you also have the option to reset your password.

Click on **New User** to create a new AMP for Endpoints Console user account. A valid email address is required for them to receive an account activation email. You can also add a different email address to receive notifications; for example, if you want all notifications you create to go to a distribution list. You must also decide if the user will be an administrator or an unprivileged user. An administrator has full control over all aspects of the AMP for Endpoints deployment. If you uncheck the **Administrator** box, the user will only be able to view data for groups you assign to them. You can also change the user's privileges later by editing their account. See Access Control for more details.



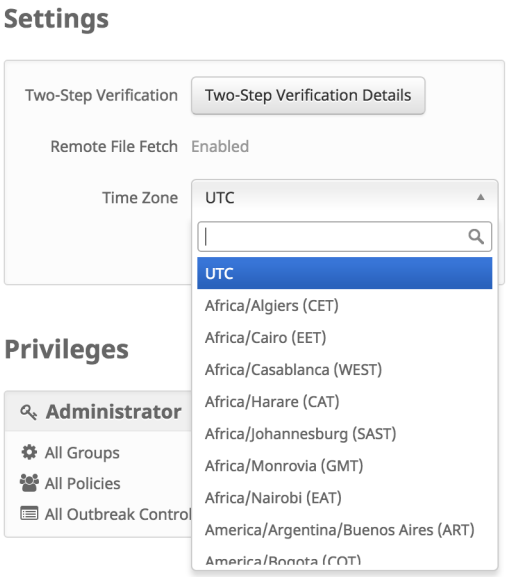
When you select a user account you can also view the subscriptions for that user. The **Subscriptions** list displays any events and reports they have subscribed to.



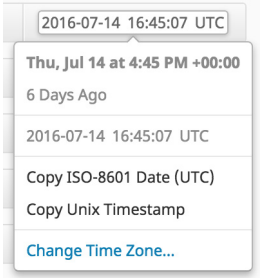
Time Zone Settings

You can change the time zone displayed by the AMP for Endpoints Console for your user account by clicking **My Account** or going to the **Users** page and clicking on your name or

email address. You can change the time zone settings at any time by going back to your account page.



If you need to see a date in UTC or other formats, click on the date and a pop-up menu will show other date options. You can also click **Change Time Zone** to go directly to your user edit page.



IMPORTANT! All Connector events will be displayed in the time zone you set and not in the local time zone of the computer that observed the event.

Access Control

There are two types of users in AMP for Endpoints, administrators and unprivileged users. When you create a new user you must select their privilege level, but you can change their access level at any time.

Administrators

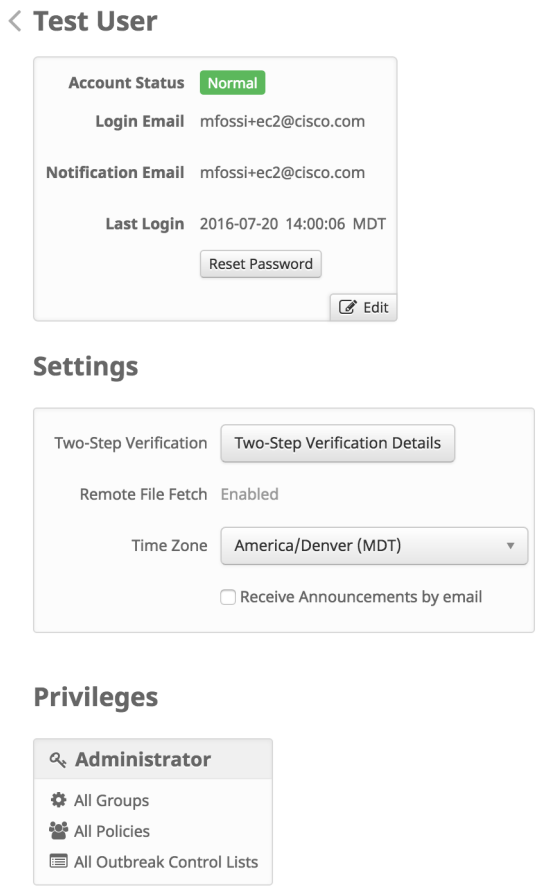
The administrator privilege allows full control over all aspects of your AMP for Endpoints deployment. Administrators can view data from any group or computer in the organization and make changes to groups, policies, lists, and users.

Only administrators can do the following:

- Create and edit Groups
- Create Policies
- Access the File Repository and fetch remote files
- Upload endpoint IOCs
- Initiate endpoint IOC scans
- Generate and view Reports
- Create new users
- Edit existing users
- Change user permissions, including granting or revoking administrator permissions
- Change Business settings
- Enable Demo Data

- View the Audit Log
- Access the **Quick Start**

IMPORTANT! An administrator can demote another administrator to a regular user but cannot demote themselves.



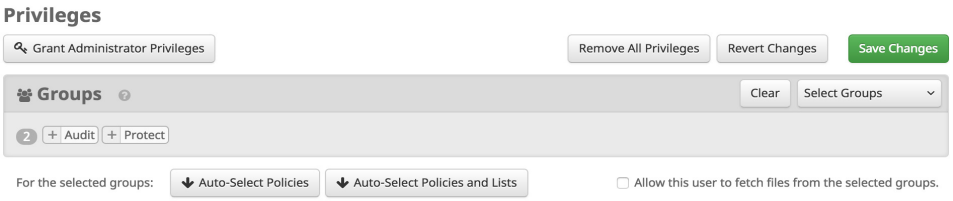
Unprivileged Users

An unprivileged or regular user can only view information for groups they have been given access to. Certain menu items will not be available to them such as Endpoint IOC scans, File Repository, and Reports.

When you create a new user, you will have the choice whether to grant them administrator privileges. If you do not grant them those privileges, you can select which groups, policies, and lists they have access to.

Start by selecting the groups you want the user to have access to. The **Clear** button removes all groups that have been added to that user. To undo changes from the current session, use the

Revert Changes button. The **Remove All Privileges** button will remove all groups, policies, and Outbreak Control lists that have been assigned to the user.



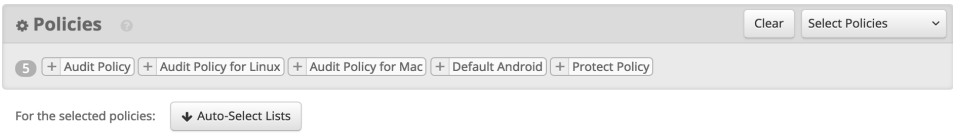
The user will be able to view these groups on the Groups page but not be able to make any changes or create new groups. The user will also be able to view information from AMP for Endpoints Connectors in these groups, such as:

- Dashboard Overview Tab, Events Tab, Heat Map Tab
- File Trajectory
- Device Trajectory
- File Analysis
- Threat Root Cause
- Prevalence
- Vulnerable Software
- IOC scans

You can also allow the user to fetch files from computers in the Groups you assign to them so they can be viewed in the File Repository. The user will need to enable Two-Step Verification before they can view the repository or request files.

IMPORTANT! Unprivileged users can only request and view files from groups they have permission to access.

Once you have selected the groups the user can access, you can select the Policies they are allowed to view and edit. You can either manually assign individual policies to the user or click one of the auto-select buttons to populate the policies and outbreak control lists associated with the groups you selected. The **Clear** button will remove all policies the user has been given access to.



Next, you can select Outbreak Control lists the same way. Either select individual lists or click the auto-select button to populate the outbreak control lists assigned to the policies you previously selected. The **Clear** button next to each list will remove only the lists of that type that have been assigned to the user.

WARNING! Exercise caution when assigning access to policies and lists. Some policies and lists can be used by other groups that the user does not have access to. This could allow the user to make changes that affect those groups.

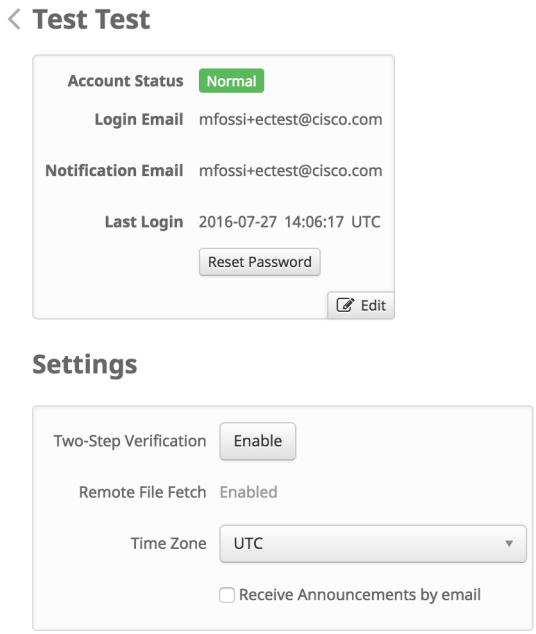
You can also modify a user's group access at any time, make them an administrator, or demote an administrator to an unprivileged user. When an unprivileged user views their own account they can view the list of groups they can access and change their own password, email addresses, or enable two-step verification.

IMPORTANT! When changing user permissions some data is cached in Search results so a user may still be able to see it for a period of time even though they no longer have access to a group. In most cases, the cache is refreshed after 5 minutes.

Two-Step Verification

Two-step verification provides an additional layer of security against unauthorized attempts to access your AMP for Endpoints Console account. It uses an RFC 6238 compatible application such as Google Authenticator to generate one-time verification codes to be used in conjunction with your password.

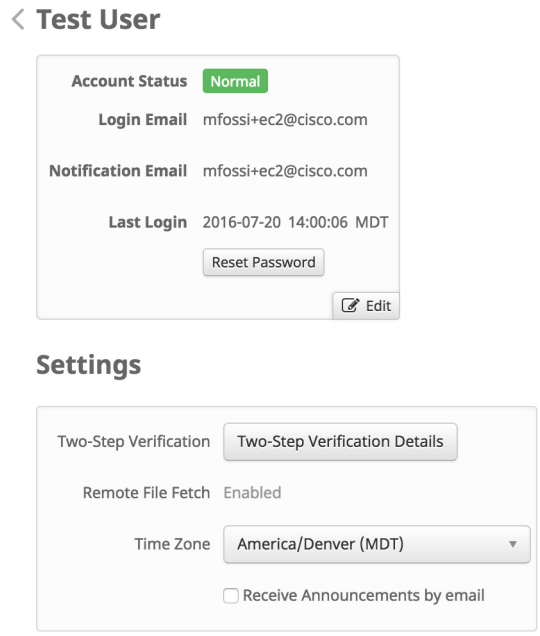
You can enable two-step verification for your account by clicking on **Enable** next to the Two-Step Verification entry on your account in the **Users** page.



You will then be guided through the steps to enable two-step verification on your account, including backup codes. It is important to keep a copy of your backup codes in a safe location in case you are unable to access the device with your authenticator app.

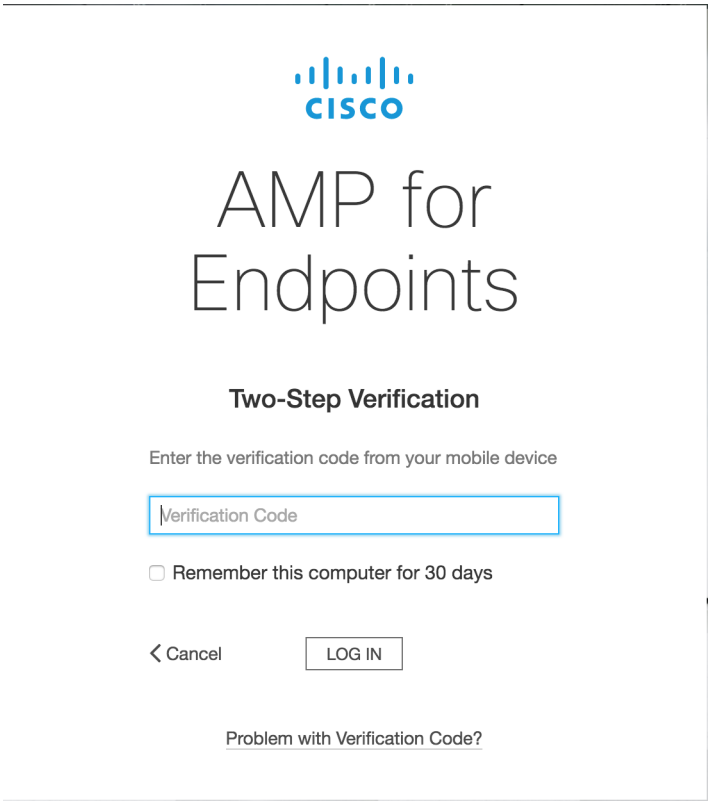
IMPORTANT! Each backup code can only be used one time. After you have used all your backup codes you should return to this page to generate new ones.

Once you have successfully enabled two-step verification on your account, you will now see a link to view **Two-Step Verification Details**.



If you need to disable two-step verification or generate new backup codes, click this link to return to the two-step verification setup page.

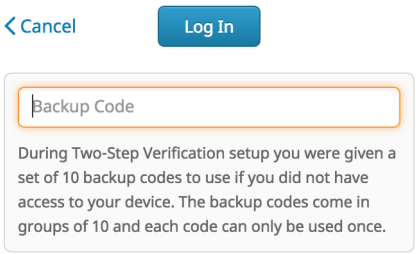
The next time you log in to the AMP for Endpoints Console you will be prompted for your verification code after you enter your email address and password.



Checking **Remember this computer for 30 days** will set a cookie that allows you to bypass two-step verification on the current computer for the next 30 days. Your browser must be set to allow cookies to use this setting.

WARNING! If you accidentally check **Remember this computer for 30 days** on a public computer, a computer you will no longer have access to, or decide to disable two-step verification, you should clear the cookies on your browser.

If you do not have access to your authenticator device, click **Can't log in with your verification code?** and enter one of your backup codes that you generated.

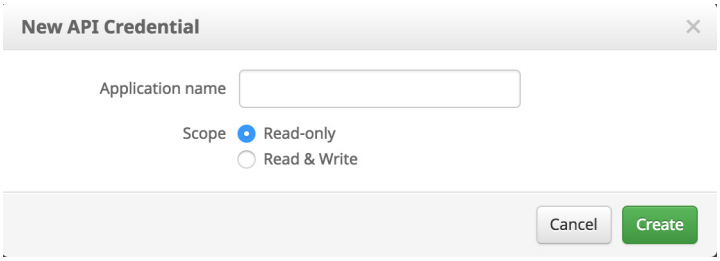


If you do not have access to your authenticator device or your backup codes, you will need to contact Support.

API Credentials

The **API Credentials** page allows you to add and remove API credentials for specific applications. For more information see the AMP for Endpoints API documentation.

Click **New API Credential** to generate an API key for your application. You can enter the name of the application for reference purposes and assign a scope of read only or read and write permissions.



IMPORTANT! An API credential with read and write scope can make changes to your AMP for Endpoints configuration that may cause significant problems with your endpoints. Some of the input protections built into the AMP for Endpoints Console do not apply to the API.

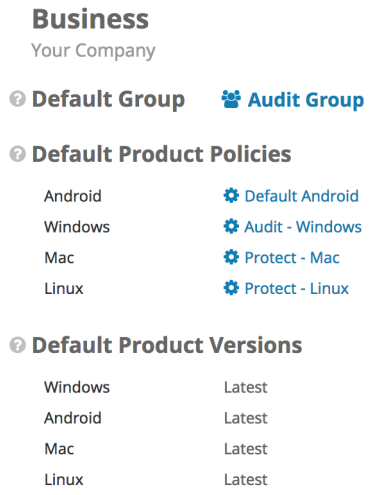
The unique API client ID and API key for the application will be displayed when you click the **Create** button. This information cannot be displayed after you leave this page so if you forget the credentials or need to change them you will have to delete the credentials and create new ones.

IMPORTANT! Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Business

The **Business** screen allows you to specify global defaults for your AMP for Endpoints deployment and displays your current license status.

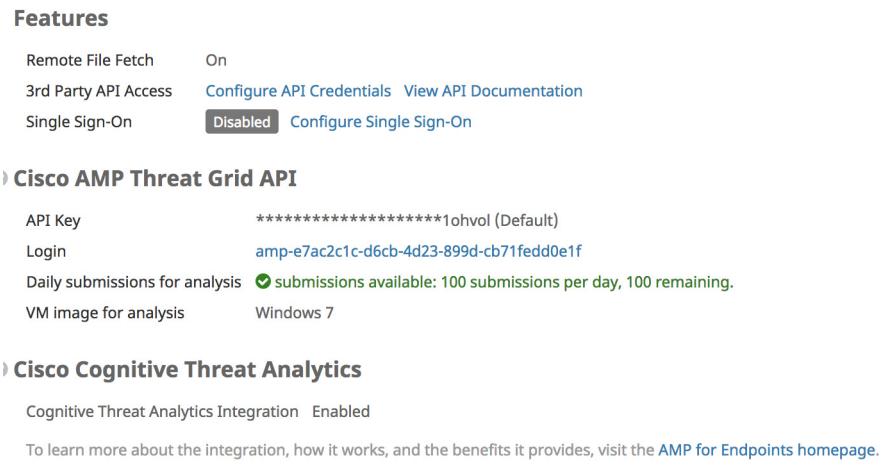
Selecting the **Default Group** or **Default Policy** from this screen will open the appropriate screen to view the details of the group or policy and edit them if desired. Click the edit link to make changes.



The **Name** entry appears on all reports that are generated from your AMP for Endpoints deployment. You can also change the **Default Group** that computers not assigned a group will be a part of. Similarly, the **Default Policy** defines the initial policy for any new groups that are created unless one is specified or they inherit one through their parent. The **Default Product Version** allows the administrator to specify which version of the AMP for Endpoints Connector will be installed during new deployments.

Features

The **Features** section of the Business page allows you to enable or disable certain features and define interaction with Cisco AMP Threat Grid.



You can disable the **Remote File Fetch** feature on this screen. To disable it, you will need to have Two-Step Verification enabled on your account and provide your verification code.

WARNING! Disabling **Remote File Fetch** will affect all AMP for Endpoints users in your business. To enable it again you will need to contact Support.

3rd Party API Access allows you to use the application programming interfaces to access your AMP for Endpoints data and events without logging into the Console. You can generate the API key from the API Credentials page. For more information, see the AMP for Endpoints API documentation.

Click to configure **Single Sign-On** for your business. This will allow your users to log in to the AMP for Endpoints Console using their single sign-on credentials once configured. You cannot use Two-Step Verification with single sign-on enabled, but all features requiring two-step verification will be enabled.

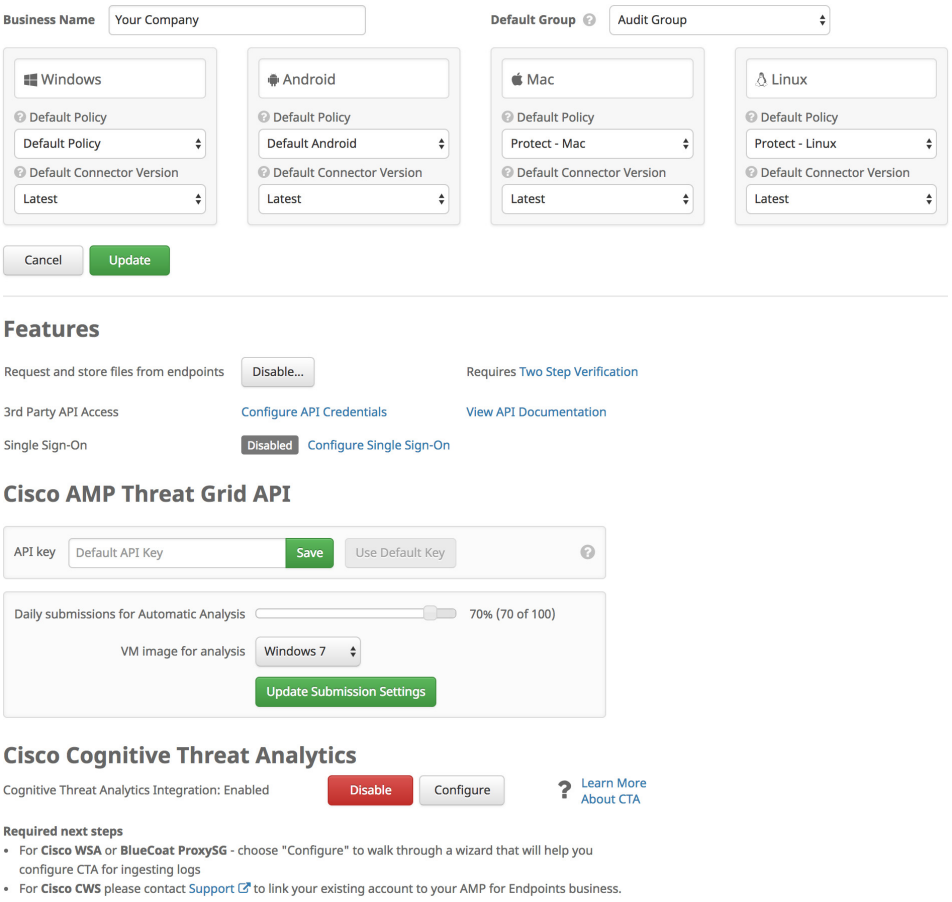
You can enter your Threat Grid API key, if you have a separate Cisco AMP Threat Grid account. This allows you to see analysis results from your Threat Grid account in File Analysis. When you enter a Threat Grid API key, the number of submissions you can make per day is displayed. If you reach the limit, you will not be able to submit files through **File Analysis** or through Automatic Analysis on the Prevalence page. If at any time you need to revert to the initial AMP Threat Grid API key that was assigned to you, click the **Use Default Key** button.

To limit the number of daily submissions used by **Automatic Analysis,** you can set the percentage of your total daily submissions using the slider. You can use up to 80% of your daily submission quota for Automatic Analysis. You can also set the default operating system that files submitted for analysis are run in with the VM image for analysis drop-down. All files submitted through Automatic Analysis will be submitted to a VM using the operating system image selected, but you can change this setting when manually submitting a file through File Analysis

Click the **Configure** button to create a Cognitive Threat Analytics account linked to your AMP for Endpoints business. This will also configure single sign-on between the two systems so that you can use your AMP for Endpoints credentials to log in to CTA. You will then be able to

configure web log uploads from AMP for Endpoints to CTA for processing. To allow unprivileged users to view CTA events, contact Support.

IMPORTANT! If you are already a Cognitive Threat Analytics customer, please contact Support to link your existing account to your AMP for Endpoints business. Otherwise, using the **Configure** button will create a separate empty CTA account..



Your current license information is displayed on the right side of the Business screen. The **License State** indicates whether or not your license is compliant, while **License Start** and **License End** display the duration of your current AMP for Endpoints license. Seats indicates how many of the seats (AMP for Endpoints Connector deployments) you have licensed are currently in use.

Single Sign-On

The AMP for Endpoints Single Sign-On (SSO) feature streamlines the user login process while enhancing security. SSO involves three parts: the user, an identity provider (IdP), and the AMP for Endpoints Console. The user connects to the Console and attempts to authenticate by entering the username. If the portal recognizes the username, it redirects the user's

authentication request to the IdP, which stores the user's information in a database. The IdP then validates the user. On successful authentication, the portal gives the user access to the portal.

You can configure the AMP for Endpoints Console to use single sign-on if you have an existing identity provider. Some providers require additional configuration steps that can be found in Single Sign-On Configurations.

Requirements

AMP for Endpoints single sign-on currently supports the SAML 2.0 standard and has been tested with the following identity providers:

- Okta
- Ping Federate
- Windows 2008 Active Directory
- Windows 2012 Active Directory

For Active Directory you must use E-Mail Address as the Outgoing Claim Type for the AMP for Endpoints console.

Configuration

To enable single sign-on for your business:

1. Log into an AMP for Endpoints administrator account.
2. Go to Accounts -> Business.
3. Click the Configure Single Sign-On link.
4. Download your SAML metadata file from your identity provider or copy the SAML metadata URL.
5. Upload the metadata file or paste the SAML metadata URL into the AMP for Endpoints console under Identity Provider Settings.
6. Click Save SAML Configuration.
7. Use the information under Service Provider Settings to configure your identity provider with the information needed to validate AMP for Endpoints.
8. Click Test to verify the connection to the service provider. If the test fails verify that your settings are correct. If it continues to fail contact Support.
9. Click Enable SAML Authentication to complete the setup.

An email will be sent to each of your AMP for Endpoints users with instructions on how to log in. Users will now have to log in by clicking the **Use Single Sign-On** link on the log in page and entering their email address. If they have not already authenticated to the identity provider they will be redirected to do so.

Caveats

When single sign-on is enabled:

- All user passwords in the AMP for Endpoints console are reset to prevent them from logging in using the standard username and password mechanism. Users will not be able to change or reset their passwords through the AMP for Endpoints console.
- Two-step verification will be disabled for each user. You will need to re-enable two-step verification if you disable single sign-on.
- Two-step verification will no longer be required to use the File Repository.
- You can create a new user with single sign-on disabled. This can be useful if your identity provider is offline or unreachable and you still need to access the AMP for Endpoints console.
- All AMP for Endpoints users must have an account with an email address that has a corresponding email address at the identity provider.
- If you have any AMP for Endpoints users who do not have a matching email address at the identity provider those users will no longer be able to log in to the console. Contact support to have single sign-on disabled for those users.
- AMP for Endpoints only supports SAML for SSO and not OAUTH.

Disable Single Sign-On

To disable single sign-on for your business:

1. Log into an AMP for Endpoints administrator account.
2. Go to **Accounts -> Business**.
3. Click the Configure Single Sign-On link.
4. Click **Disable SAML Authentication** to disable single sign-on.

A password reset email will be sent to all single sign-on users in your business who had single sign-on enabled. Users will have to reset their password before they can log in to the AMP for Endpoints console.

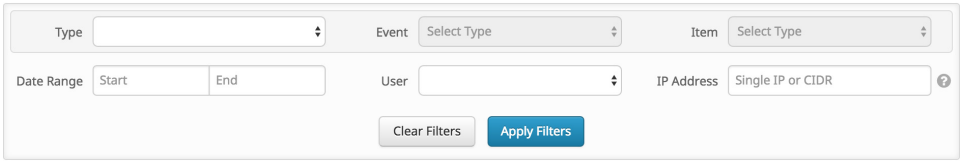
Audit Log

The audit log allows the AMP for Endpoints administrator to track administrative events within the Console that may affect other Console users. Actions such as account creations, deletions, password resets, user login, user logout, creation and deletion of reports, policy changes, and other actions are all tracked. Associated information with each entry includes the date, the object acted on, action, changes that were made (if applicable), messages associated with the action, the user who triggered the action, and the IP address they were connected from.

You can filter the audit log to show certain event types, date ranges, users, or IP addresses. The **Type** includes items such as policies, groups, outbreak control lists, and users. Once you select

a type you can select an event specific to the Event type, like creation, deletion, and updates. The **Item** includes specific lists, computers, groups, and users.

IMPORTANT! Item lists with more than 5000 computers cannot be displayed in the pull-down menu. Go to Computer Management and locate the computer you want to see the audit log for using the filters, then click the **View Changes** link for that computer to see a filtered view of the audit log.



Each audit log event can be expanded to show more information on the specific event including the user who generated the event, the IP address of the computer they were logged into at the time, and the time and date.

Demo Data

Demo Data allows you to see how AMP for Endpoints works by populating your Console with replayed data from actual malware infections. This is useful for evaluating the product and demonstrating its capabilities without having to infect computers yourself.

Enabling Demo Data will add computers and events to your AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, Detections, and Events behave when malware is detected. Demo Data can coexist with live data from your AMP for Endpoints deployment; however, because of the severity of some of the Demo Data malware, it may obscure real events in certain views, such as the Dashboard Indications of Compromise widget.

Click on **Enable Demo Data** to populate your Console with the data.

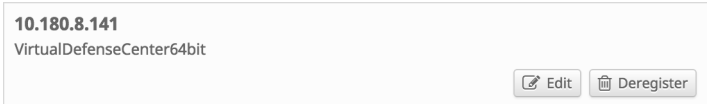
When the Demo Data has been enabled you can click **Disable Demo Data** to remove it again.

Refresh Demo Data is similar to enabling it. When Demo Data is enabled, refreshing it will simply refresh all the events so that they appear in the current day's events.

IMPORTANT! It can take up to one hour for demo data to appear in the Incidents of Compromise dashboard widget. If you disable Demo Data before it has finished populating, some events may still appear afterward. You will need to enable Demo Data again then wait at least an hour before disabling it to remove these events.

Applications

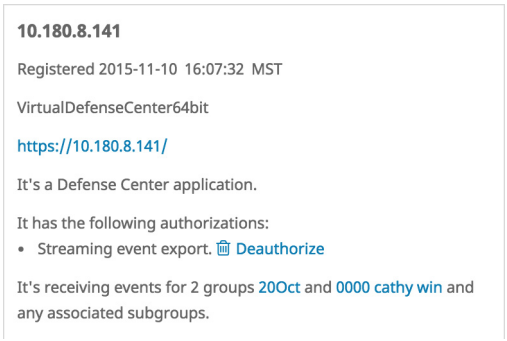
The **Applications** menu shows which applications external to AMP for Endpoints you have authorized to access your organization's data. For example, you can display AMP for Endpoints data in your **Cisco Defense Center** dashboard. For more information on Defense Center integration with AMP for Endpoints, see your Defense Center documentation.



From this page you can view your application settings by clicking on its name, edit the groups that are sending data to the application, or deregister the application from AMP for Endpoints entirely.

Application Settings

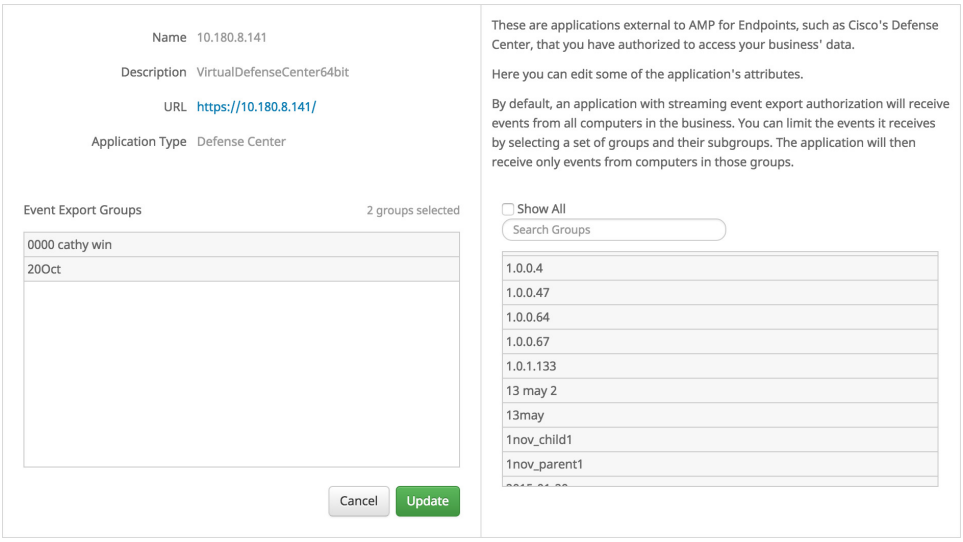
When you select the name of an application from your list you will see the current settings for that application.



The type of application, its authorizations, and the groups it is receiving events for are displayed. From this view, you can also deauthorize any data streams the device is receiving.

Edit an Application

By default, an application with the **streaming event export authorization** will receive events from all groups in your organization.



If you want to exert more granular control over the events sent from your AMP for Endpoints deployment to the application, select one or more groups from the list on the right. If you want to remove a group, select it from the Event Export Groups list on the left. If the Event Export Groups list is empty, the application will receive events from all computers across all groups in your organizations. To stop the application from receiving events from AMP for Endpoints entirely, you must deregister it from the main Applications screen.

APPENDIX A
THREAT DESCRIPTIONS

AMP for Endpoints has unique network detection event types and Indications of Compromise. Descriptions of these detection types are found in this section.

IMPORTANT!For descriptions of threat names, see AMP Naming Conventions.

Indications of Compromise

AMP for Endpoints calculates devices with Indications of Compromise based on events observed over the last 7 days. Events such as malicious file detections, a parent file repeatedly downloading a malicious file (Potential Dropper Infection), or multiple parent files downloading malicious files (Multiple Infected Files) are all contributing factors. Indications of compromise include:

- Threat Detected - One or more malware detections were triggered on the computer.
- Potential Dropper Infection - Potential dropper infections indicate a single file is repeatedly attempting to download malware onto a computer.
- Multiple Infected Files - Multiple infected files indicate multiple files on a computer are attempting to download malware.
- Executed Malware - A known malware sample was executed on the computer. This can be more severe than a simple threat detection because the malware potentially executed its payload.
- Suspected botnet connection - The computer made outbound connections to a suspected botnet command and control system.
- [Application] Compromise - A suspicious portable executable file was downloaded and executed by the application named, for example Adobe Reader Compromise.

- [Application] launched a shell - The application named executed an unknown application, which in turn launched a command shell, for example Java launched a shell.
- Generic IOC - Suspicious behavior that indicates possible compromise of the computer.
- Suspicious download - Attempted download of an executable file from a suspicious URL. This does not necessarily mean that the URL or the file is malicious, or that the endpoint is definitely compromised. It indicates a need for further investigation into the context of the download and the downloading application to understand the exact nature of this operation.
- Suspicious Cscript Launch - Internet Explorer launched a Command Prompt, which executed cscript.exe (Windows Script Host). This sequence of events is generally indicative of a browser sandbox escape ultimately resulting in execution of a malicious Visual Basic script.
- Suspected ransomware - File names containing certain patterns associated with known ransomware were observed on the computer. For example, files named help_decrypt.<filename> were detected.
- Possible webshell - the IIS Worker Process (w3wp) launched another process such as powershell.exe. This could indicate that the computer was compromised and remote access has been granted to the attacker.
- Cognitive Threat - Cisco Cognitive Threat Analytics uses advanced algorithms, machine learning, and artificial intelligence to correlate network traffic generated by your users and network devices to identify command-and-control traffic, data exfiltration, and malicious applications. A Cognitive Threat Indication of Compromise event is generated when suspicious or anomalous traffic is detected in your organization. Only threats that CTA has assigned a severity of 7 or higher are sent to AMP for Endpoints.

IMPORTANT! In certain cases the activities of legitimate applications may trigger an Indication of Compromise. The legitimate application is not quarantined or blocked, but to prevent another Indication of Compromise being triggered on future use you can add the application to Application Control - Whitelisting.

DFC Detections

Device Flow Correlation allows you to flag or block suspicious network activity. You can use Policies to specify AMP for Endpoints Connector behavior when a suspicious connection is detected and also whether the Connector should use addresses in the Cisco Intelligence Feed, custom IP lists you create, or a combination of both. DFC detections include:

- DFC.CustomIPList - The computer made a connection to an IP address you have defined in a DFC IP Black List.
- Infected.Bothost.LowRisk - The computer made a connection to an IP address thought to belong to a computer that is a known participant in a botnet.
- CnC.Host.MediumRisk - The computer made a connection to an IP address that was previously known to be used as a bot command and control channel. Check the Device Trajectory for this computer to see if any files were downloaded and subsequently executed from this host.

- ZeroAccess.CnC.HighRisk - The computer made a connection to a known ZeroAccess command and control channel.
- Zbot.P2PCnC.HighRisk - The computer made a connection to a known Zbot peer using its peer-to-peer command and control channel.
- Phishing.Hoster.MediumRisk - The computer made a connection to an IP address that may host a phishing site. Often, computers phishing sites also host many other websites and the connection may have been made to one of these other benign sites.

APPENDIX B
SUPPORTING DOCUMENTS

The following supporting documents are available for download.

Cisco AMP for Endpoints User Guide

The current version of the User Guide can be downloaded here.

Download the User Guide

Cisco AMP for Endpoints Quick Start Guide

This guide walks through setting up groups, policies, and exclusions then deploying AMP for Endpoints Connectors. This guide is useful for evaluating AMP for Endpoints.

Download the Quick Start Guide

Cisco AMP for Endpoints Deployment Strategy Guide

This guide provides a more detailed look at preparing and planning for a production deployment of AMP for Endpoints along with best practices and troubleshooting tips.

Download the Deployment Strategy Guide

Cisco Endpoint IOC Attributes

The Endpoint IOC Attributes document details IOC attributes supported by the Endpoint IOC scanner included in the AMP for Endpoints Connector. Sample IOC documents that can be uploaded to your AMP for Endpoints Console are also included.

Download the Endpoint IOC Attributes

Cisco AMP for Endpoints API Documentation

The API allows you to access your AMP for Endpoints data and events without logging into the Console. The documentation provides descriptions of available interfaces, parameters, and examples.

View the API documentation

Cisco AMP for Endpoints Release Notes

The Release Notes contain the AMP for Endpoints change log.

Download the Release Notes

Cisco AMP for Endpoints Demo Data Stories

The Demo Data stories describe some of the samples that are shown when Demo Data is enabled in AMP for Endpoints.

Download the SFEICAR document

Download the ZAccess document

Download the ZBot document

Download the CozyDuke document

Download the Upatre document

Download the PlugX document

Download the Cryptowall document

Download the Low Prevalence Executable document

Download the Command Line Capture document

Download the Cognitive Threat Analytics (CTA) document

Download the WannaCry Ransomware document

Single Sign-On Configurations

Some identity providers require additional configuration steps to enable single sign-on with the AMP for Endpoints Console. See the documents below for instructions.

Download the Active Directory setup guide

Download the Okta setup guide

Download the Ping Federate setup guide

Cisco Universal Cloud Agreement

Cloud Offer Terms

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

Z