Secure Endpoint User Guide

Last Updated: October 19, 2023

Table of Contents

Chapter 1
Dashboard

The Secure Endpoint (formerly 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.

Console System Requirements

To access the Secure Endpoint console, you will need one of the following Web browsers:

- Microsoft Edge 88 or higher
- Mozilla Firefox 81 or higher
- Apple Safari 14 or higher
- Google Chrome 86 or higher

Organization Switcher

The organization switcher allows you to quickly change between Secure Endpoint organizations. You must have accounts in each organization to switch between them. The organization switcher will only be visible If you have accounts in multiple organizations. The name of the current organization is displayed in the ribbon.

To switch to another organization:

1. Click the Switch button to display the list of organizations.
2. Select the organization you want to access.

IMPORTANT! The organization switcher is a great feature of Secure Endpoint that allows a user belong to multiple organizations and switch between them. However, there can be some unexpected behavior related to this. When you first log in to Cisco XDR, SecureX, or Orbital, you are assigned a session for the Secure Endpoint organization that you are logged in to. If you switch organizations in Secure Endpoint, the organization is NOT switched in Orbital or SecureX. To switch organizations in Cisco XDR, Orbital or SecureX, you must log out of those systems, then log in again and select the organization you want to use.

Threat Severity

Threat severity is represented by color-coded tags that appear in the interface on pages such as the Dashboard Tab, Inbox Tab, and Events Tab to provide quick insight into the most important compromises.

Threat severity also appears in the Inbox Tab interface as color-coded mini-bar graphs which summarize the relative number of events. You can hover the mouse cursor over the graphs to display a detailed view.

Threat severity levels assigned to individual event types are evaluated by Cisco's threat research team and may vary depending on how threats appear in combination with each other.

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:

- Global threat alerts in your environment, if you have configured it in the Features for your organization.
- Automated submissions and retroactive threat detections through Secure Malware Analytics (formerly 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 Secure Endpoint connectors.

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

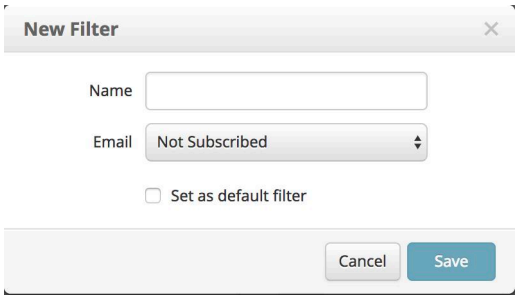
- Links to the Quick Start setup for each connector type.

Filters

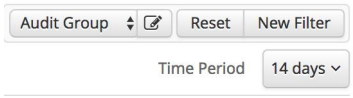
You can filter activity by designated group, time period (the past 14 days, 7 days, 1 day, or 1 hour), date/time selection, compromise-specific observables and compromise event types.

Each of these filters may be applied alone or as a combination of filters. Compromise observables 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, observables, 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.



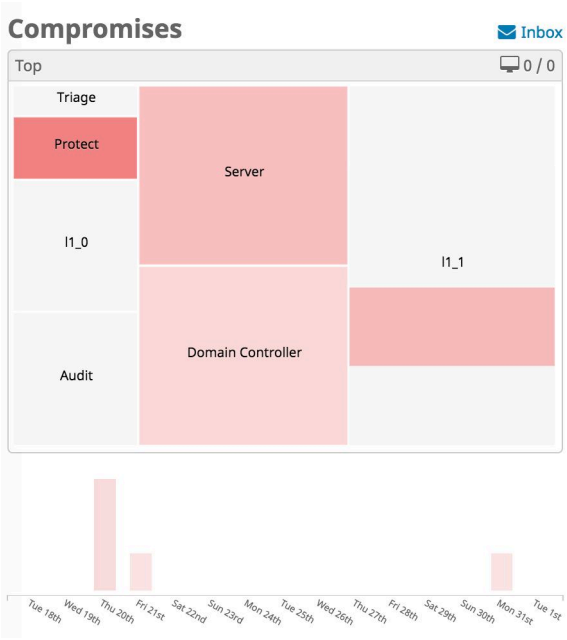
Once you have saved a custom filter you can select it from the drop down, edit the selected filter, or reset the view to the default with no filters applied.



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 Secure Endpoint 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 observable, 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 Observables

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

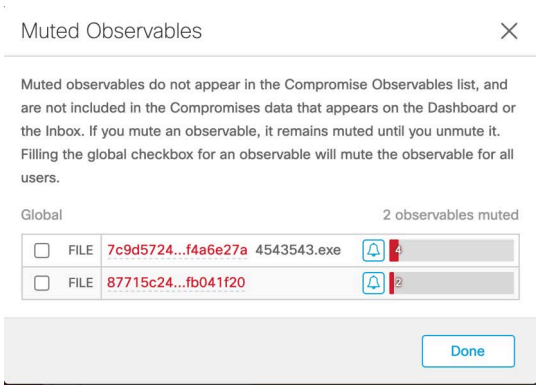
Click on the first (FILE, URL, IP) or last column (with the red bar), or filename in the second column of a compromise observable to filter compromise-related data on the Dashboard and Inbox view by the selected observable.

The resulting view will exclude data for all other observables in the % compromised, Compromises, and Compromise Event Types.

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

You can mute an observable type by clicking the bell icon so that the Dashboard or Inbox won't show data associated with it.

You can also manage the muted observables by clicking on the cog icon.



Unmute the observable by clicking on the bell icon. Unless the global checkbox is filled, muting of observables will only affect the user account for which the change was made. You can mute the observable for all user accounts by filling the global checkbox. You can add an explanation for globally muting the event after filling the checkbox.

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

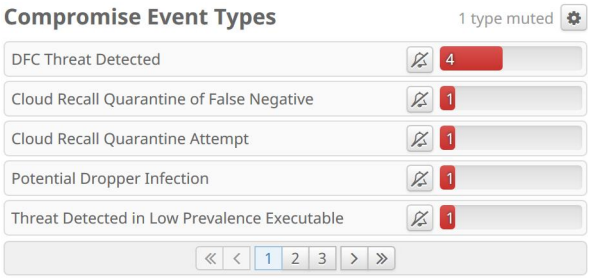
You can also quickly view information and access commonly used functions in a popup by clicking directly on an observable in the second column (such as IP address, URL, or file SHA-256). The type of observable selected determines the information displayed in the popup.

TIP! Popups aren't limited to the Dashboard tab. You can click observables anywhere in the Console interface to display a popup.

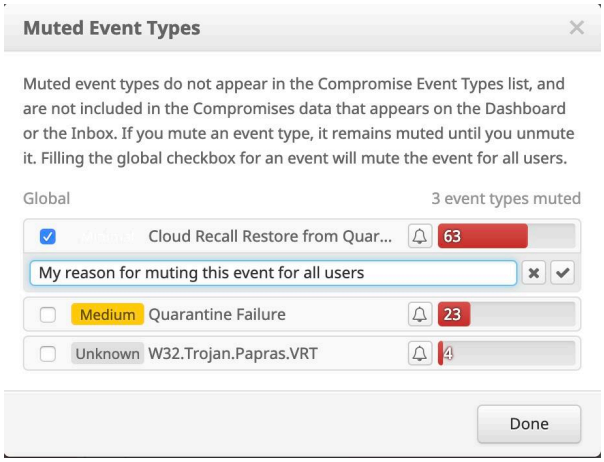
Compromise Event Types

Compromise event types describe events that Secure Endpoint 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.

You can mute an event type by clicking the bell icon so the Dashboard or Inbox won't show data associated with it.



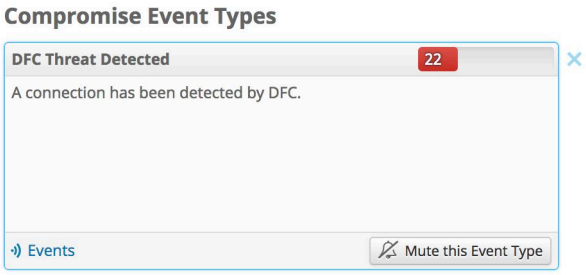
You can also view the event types that are muted by clicking the cog icon.



Unmute the event type by clicking the bell icon. Unless the global checkbox is filled, muting of events will only affect the user account for which the change was made. You can mute the event for all user accounts by filling the global checkbox. You can add an explanation for globally muting the event after filling the checkbox.

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 Observables 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.

If the event type is an indication of compromise the description of the IOC will be displayed along with the tactics and techniques associated with it. Click the Indicators link to see a filtered view of the Indicators page.

Quarantined Detections

Quarantined detections are potential compromises or malicious events that were detected and successfully quarantined so do not require any additional attention. 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. From there you can restore any files that you feel were quarantined by mistake.

IMPORTANT! Files remain in quarantine for 30 days and after that cannot be restored.

Vulnerabilities

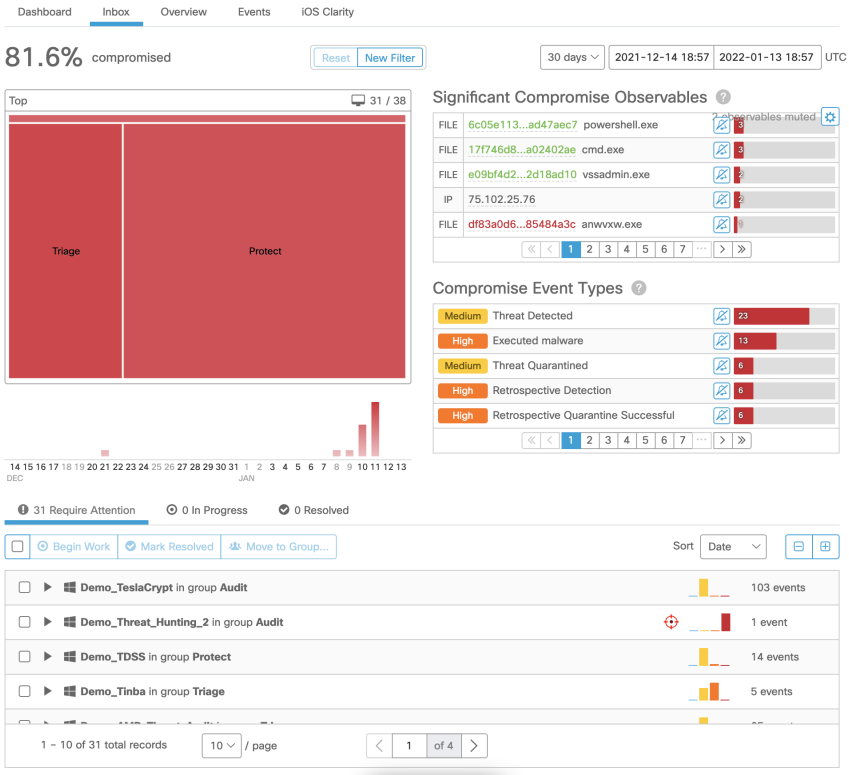
Vulnerabilities are displayed through a heat map that shows groups that include computers with known vulnerable applications installed.

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 organization 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 Observables 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 by clicking on the matching tabs. You can order the list by date or

severity by selecting from the Sort drop-down menu. 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 30 days. You will not be able to see any compromises older than 30 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 event types by clicking on the bell icons or unmute them by clicking the cog icon which appears when there are muted events.

If you have global threat alerts enabled from the Organization Settings page you will also see the number of agentless global threat alerts across your organization. Click on

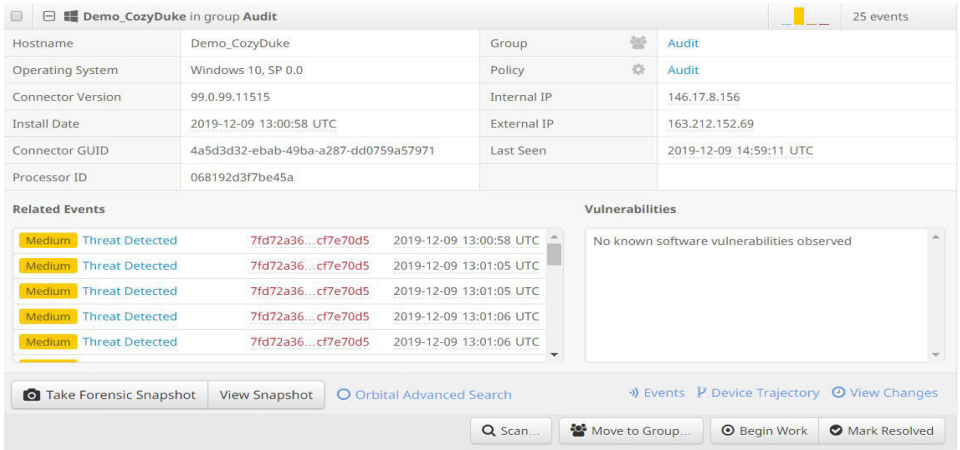
this link to view a list of devices and incidents on the Agentless Global Threat Alerts page.

IMPORTANT! If your inbox is filtered by Significant Compromise Observables and you click Mark Resolved for multiple computers, any computers with more than one observable will not be resolved. You must resolve those computers individually as multiple observables 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, initiating diagnostics (see Computer Management: Connector Diagnostics), 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 organization 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 Secure Endpoint to resolve incidents see Cisco Secure Endpoint Demo Data Stories.

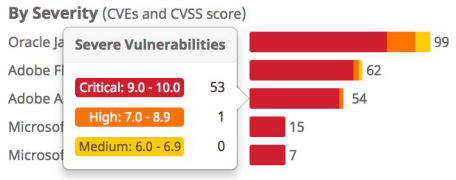
Overview Tab

The **Overview** tab displays the status of your environment and highlights recent threats and malicious activity in your Secure Endpoint deployment. You can click on the headings of each section to navigate directly to relevant pages in the console to investigate and remedy situations:

- Compromises links to Inbox Tab
- Computers links to Computers
- AV Definition Status links to AV Definition Summary
- Threats links to Dashboard Tab (filtered by Threat Detected)
- Network Threats links to Dashboard Tab (filtered by Device Flow Correlation Threat Detected, Global Threat Alerts, and iOS Network Detection)
- Vulnerabilities links to Vulnerable Software
- File Analysis links to File Analysis

Clicking any of the blue items in each of the sections also navigates directly to the relevant pages in the console.

You can hover the mouse cursor over stacked bar graphs to display a more detailed view of the data.



You can also filter the displayed data by selecting from the Groups drop-down menu in the top-right corner of the page. 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. Click the drop-down menu attached to the button to 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.

IMPORTANT! You can view muted event types in the Compromise section of the Overview tab by clicking the cog button which appears when there are muted events.

Events Tab

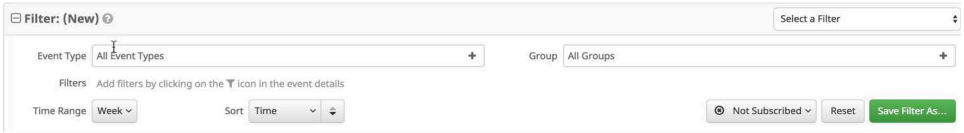
The **Events** tab initially shows the most recent events in your Secure Endpoint deployment. Navigating to the **Events** tab by clicking on a threat, IP address, or computer name in the **Dashboard** tab will provide different filtered views.

Filters and Subscriptions

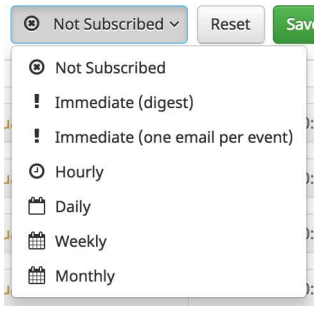
Filters are shown at the top of the Events tab. You can select a previously saved filter from the drop-down on the right side or add event types, groups, or specific filters from existing events. To remove a filter criteria, click the x next to the item you want to remove. You can also sort the Events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

Clicking on a SHA-256 in the Secure Endpoint console will display a 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.

IMPORTANT! When Casebook is enabled, the SHA-256 File Info Context Menu is replaced by the Pivot Menu.

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 or submit it for File Analysis.

The Outbreak Control sub-menu also allows you to quickly add the SHA-256 to one of your outbreak control lists. Options are available here to add the SHA-256 to new or existing Simple, Blocked Lists, or Allowed Lists.

Investigate in Cisco Threat Response will take you to the listing for the file, URL, or IP address in Cisco Threat Response.

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

Event List

The event list 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. Files remain in quarantine for 30 days and after that cannot be restored.

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 request events in CSV files. You will receive an email with a link to download an archive file containing the CSV files when it is generated. You can also use the API with an application like Splunk to create an event stream for large numbers of events.

IMPORTANT! You will get the option to cancel and restart the request if you click the Export to CSV button again while a previously requested CSV file is still being generated.

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.

Behavioral Protection Event

Events generated by the Behavioral Protection engine include additional information. Any Indicators associated with the detection will be listed in the Tactics and Techniques fields. The rest of the event is made up of three sections.

Observables

Any files, hosts, and IP addresses involved in the event will be listed. You can initiate a request to upload any observed files to the File Repository for analysis. There are also links to File Trajectory and Device Trajectory wherever applicable.

Observed Activity

This provides a summary of all the activity that was part of the detected attack. It includes file, process, registry, and network events around the detection that you can use as part of your incident response analysis.

Action

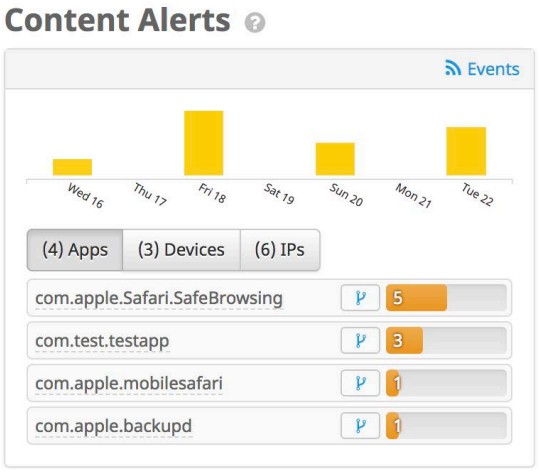
Actions (if any) performed by the connector on components of the event and the outcome of the action are listed. Actions include file quarantines, ending processes, and uploading files for analysis. Actions will only be taken if Behavioral Protection is in Protect mode.

iOS Clarity Tab

Navigate to the **Dashboard** and select the **iOS Clarity** tab. If you have already linked your Meraki SM or other Mobile Device Manager (MDM) this tab displays a summary of activity, a list of the most recently observed applications on your managed iOS devices, and a list of devices that have not reported back in more than 7 days.

Content Alerts

Content Alerts provides a brief overview of malicious and blocked sites that were observed in the last 7 days. These alerts are generated whether the Conviction Modes on the device is set to Audit, Block, or Active Block. You can click the Events link to see a filtered view of the Events Tab showing only these events.



The **Apps** tab shows the top five apps on your devices were observed connecting to malicious IPs or addresses from IP Blocked Lists and how many times each app attempted a connection in the last 7 days. You can click the name of any app to view a context menu showing the app name and publisher along with other options, including a link to the Mobile App Trajectory for that app.

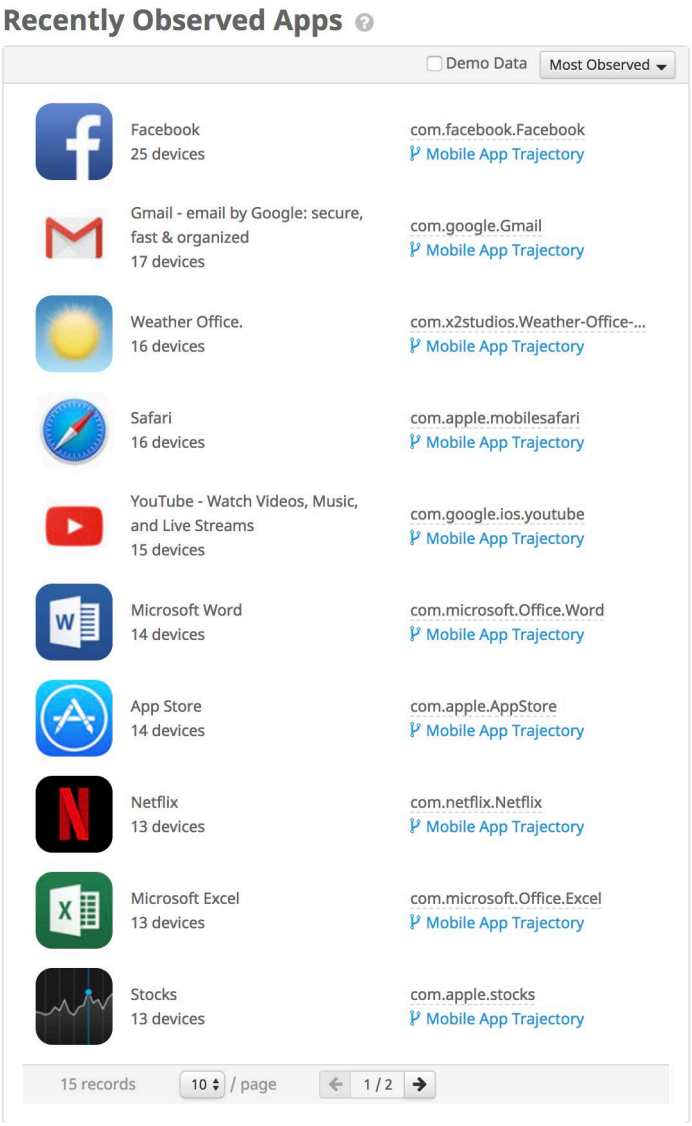
The **Devices** tabs shows the top five devices that attempted to connect to malicious IPs or addresses from IP Blocked Lists and how many times each device attempted a connection in the last 7 days. There are also icons that will take you to a filtered view of the Events Tab for that device and the Device Trajectory.

The **IPs** tab shows the top five malicious or blocked IP addresses that your devices attempted to connect to in the last 7 days. You can click an IP address to view details including Virus Total results or you can investigate the file in Cisco Threat Response.

Recently Observed Apps

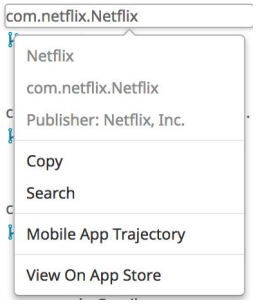
The **Recently Observed Apps** list displays the name of the app, number of devices it was observed on, the bundle ID, and a link to view the app in the Mobile App

Trajectory. You can also switch views between **Real Data** from your organization and **Demo Data**.



Click the bundle ID to activate a menu that displays the app name, package name, and publisher name. You can also copy the package name or search your Secure Endpoint

data for other apps with matching activity. You can click any bundle ID displayed in the Secure Endpoint Console to show this menu.



Unseen Devices

Unseen Devices shows iOS devices that have not reported back in 7 days or more. If more than 10 devices are in the list they will be summarized by group. Click a group name to see a filtered view of the **Computers** page showing a list of devices that have not reported in more than 7 days.

Chapter 2
Outbreak Control

Secure Endpoint 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, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists. These will be discussed in the sections that follow.

Custom Detections - Simple

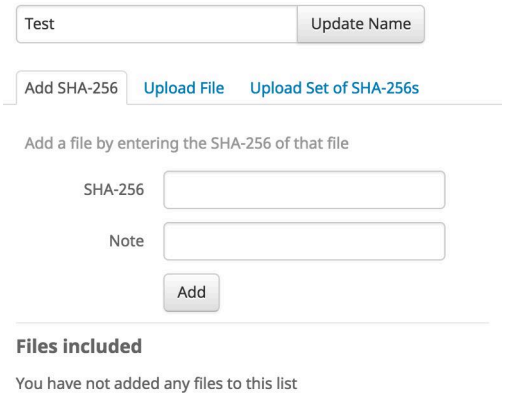
A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Not only will an entry in a Simple Custom Detection list quarantine future files, but through Retrospective it will quarantine instances of the file on any endpoints in your organization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

After you save the Simple Custom Detection, 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. 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 **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 as specified under the Cache tab in your Policies. The default 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 allowed list 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 https://docs.clamav.net/manual/Signatures.html. 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 **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 **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, it is subject to caching for an 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.

IMPORTANT! Advanced Custom Detections only work on files of unknown disposition.

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 **Save**.

After you save the custom detection, click **Edit** and you can add an app by uploading its APK file. 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 - Blocked Applications

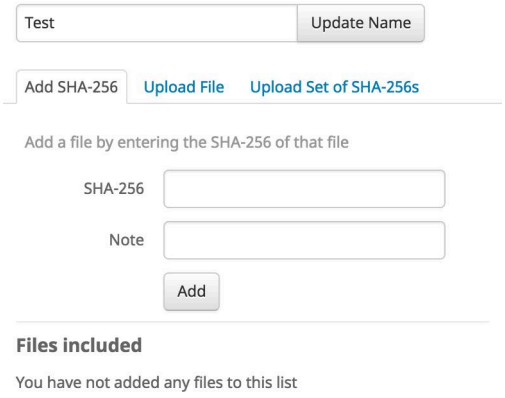
A blocked applications list is composed of files that you do not want to allow users to execute but do not want to quarantine. You may want to use this for files you are not sure are malware, unauthorized applications, or you may want to use this to stop applications with vulnerabilities from executing until a patch has been released.

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

In order to create an blocked applications list, go to **Outbreak Control > Blocked Applications**. Click **Create** to create a new blocked applications list, give it a name, and click on **Save**.

After you save the blocked applications 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 be 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 a blocked applications 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 blocked application 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 and the length of time specified under the Cache tab in your Policies. The default values are as follows:

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

If a file is added to an blocked applications 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 blocked application entries. Click **View Changes** next to a single blocked application list to view the Audit Log with all records filtered to show only the records for that specific blocked list.

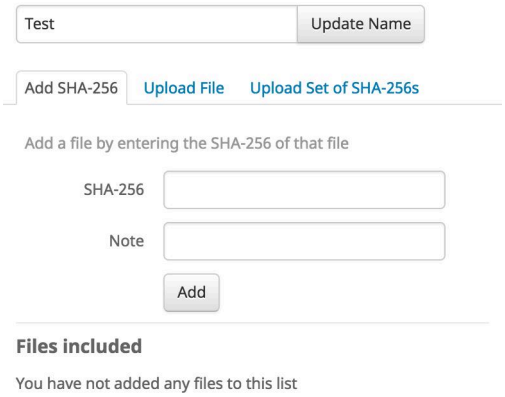
Application Control - Allowed Applications

Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company.

To create an allowed applications list, go to **Outbreak Control > Allowed Applications**. Next click **Create** to create a new allowed applications list, give it a name, and click **Save**.

After you save the allowed applications list, 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. You can see the SHA-256s and notes by clicking 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 allowed applications list entries. Click **View Changes** next to a single allowed applications list to view the Audit Log with all records filtered to show only the records for that specific allowed list.

Network - IP Block & Allow Lists

IP block and allow lists are used with device flow correlation 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 add a port to a block or allow list 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 block and allow list 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 Block Lists

An IP block list allows you to specify IP addresses you want to detect any time one of your computers connects to them. You can choose to add single IP addresses, entire CIDR blocks, or specify IP addresses with port numbers. 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 section of your policy.

IP Allow Lists

An IP allow list enables you to specify IP addresses you never want to detect. Entries in your IP allowed list will override your IP blocked list as well as the Cisco Intelligence Feed. You can choose to add single IP addresses, entire CIDR blocks, or specify IP addresses with port numbers.

IP Isolation Allow Lists

An IP isolation allow list lets you specify IP addresses that the Secure Endpoint Windows and Mac connectors will not block when an endpoint is isolated. This allows the endpoint to communicate with trusted locations within your network for further investigation during an active Endpoint Isolation session. You can add up to 200 IPV4 addresses to this list. IP isolation allow lists do not support port numbers.

IMPORTANT! By default, all Secure Endpoint Cloud addresses are included in the allow list so the connector can receive policy updates, perform cloud lookups, and update the isolation status.

Creating IP Block and Allow Lists

To create an IP list, navigate to **Outbreak Control > IP Block & Allow Lists** and click Create IP List... This displays the New IP List page. Enter the name and description for the new list and select Allow, Block, or Isolation Allow from the List Type drop-down list. You can enter one IP address or CIDR block per row. You can add single rows by clicking Add Row. You can also quickly add multiple IP addresses and CIDR blocks by clicking Add Multiple Rows... You can then enter or paste a list of IP addresses and CIDR blocks into the following dialog, then click Add Rows when you are done.

You can also upload a CSV file containing IP addresses and CIDR blocks separated by newline characters. To upload the file, click Upload..., click Browse to select the CSV file, and click Upload.

Editing IP Block and Allow Lists

To edit an IP list, navigate to **Outbreak Control > IP Block & Allow Lists**. Click the + next to the IP list you want to edit to expand the view. Click Edit. If there are fewer than 500 items on the list, you will see the default list editor to edit, add and remove rows. If there are 500 or more items on the list, you will see the long list editor which enables you to easily navigate and edit large lists, but does not include live input validation.

When you are finished, click Save. If you are using the long list editor, any invalid items will appear in the IPs / CIDR Blocks with Errors list where you can edit the items before attempting to save the list again.

IMPORTANT! You can click Revert Changes at any time to restore the IP list to its unedited state.

Exporting and Replacing Block and Allow Lists

You can also download a CSV file containing the list of IP addresses and CIDR blocks to work with offline. To download a list, expand the view of the IP list you want to download, then click Export.

To upload and replace an existing list, expand the view of the IP list you want to upload, then click Replace... Click Browse to select the file containing the list, then click Replace.

Chapter 3
Device Control

Device Control lets you view and have control over the usage of USB devices, including Windows Portable Devices (WPD) across your organization. With visibility, you can see the devices connected to endpoints. For instance, when investigating a compromise in device trajectory, you can see device control events like blocked devices. Such events can also be filtered and visualized within the events page.

With granular control, you can create rules so that only approved USB devices are used in your environments. As organizations have their own preferences on how to manage USB devices, Secure Endpoint offers granular rules that can support a variety of configurations and use cases.

For instance, you can define general policies (e.g. block read/write/execute), while creating granular rules that allow certain types of devices based on device properties. Rules can be re-ordered to adjust for the desired order of enforcement, and are assigned to policies, allowing for a balance between ease of management (with shared rule sets across policies) or granular control (with different rule sets for each policy and group).

Only administrators can create a new Device Control configuration. Unprivileged users can manage configurations they have been given permission to in Access Control. They are able to add, update, delete, and reorder rules in a configuration and add configurations to policies they can access.

IMPORTANT! Device Control is available for Secure Endpoint Windows connector 8.1.3 and later, with WPD support for 8.2.1 and later.

Device Control configurations and rules

Device Control rules are part of a configuration. A Device Control configuration is added to a policy so they will be processed by endpoints in the groups that use that policy.

There is no audit mode for Device Configuration. A configuration for Device Control can be created to only collect USB mass storage devices and WPDs that are attached and do not restrict access to the device. Create a configuration with a Base Rule of Read, Write and Execute. All USB mass storage devices and WPDs will be allowed and events visible on the Events page and in Device Trajectory.

IMPORTANT! There is no option for Read, Write, and Execute for WPD because execute is currently unsupported.

Create a Device Control configuration

Only administrators can create new Device Control configurations.

1. Navigate to Management -> Device Control.
2. Click **New Configuration**.
3. Enter a unique name for the configuration.
4. Enter a description for the configuration (optional).
5. Select USB Mass Storage or Windows Portable Device.
6. Select a base rule permission. See Device Control permissions for descriptions of each permission.
7. Select whether notifications should be displayed on the endpoint when a Device Control rule is triggered.

   IMPORTANT! For Secure Endpoint Windows connector 8.1.3 Engine Notifications under Client User Interface must be enabled in the policy for notifications to be displayed on the endpoint. This is not required for version 8.1.5 and later.

8. Click Save.

A configuration without any rules will affect all devices of the configuration type. Add rules to your configuration for additional granularity to allow or block specific USB mass storage devices. For example, you could create a configuration that blocks all USB mass storage devices but allows read and write access to devices from a specific vendor.

Add a rule to the configuration

You can add up to 1000 rules to a single configuration. You will need at least one of the following identifiers to create a rule:

Identifier

Criteria	Description
Vendor name	Also known as the manufacturer name.
Vendor ID	A 4-digit code that is assigned to a vendor by the usb committee. Common use cases: block or allow devices from a specific vendor across multiple endpoints.
Product name	Also known as the friendly name or device name.
Product ID	A 4-digit code that is assigned to the specific product by the vendor. Common use cases: block or allow devices for a model/type of device across multiple endpoints.
Instance ID	A unique identifier composed of vendor ID and product ID. Common use cases: block or a allow a specific device in the context of a specific endpoint (not across endpoints).
Device ID	The first part of instance ID that contains the vendor ID and product ID. Common use cases: block or allow a specific USB device across multiple endpoints.

IMPORTANT! Serial numbers are not used as criteria because they are an optional field for USB manufacturers and therefore unreliable.

You can add a rule to a configuration from the Device Control page, from a Device Control event on the Event List, or from a Device Control event in Device Trajectory.

To create a rule for your configuration:

1. Click the name of the configuration or the edit configuration button under Actions.
2. Click Add Rule.
3. Enter a description for the rule (optional).
4. Select if Any or All of the criteria need to be met to trigger the rule. Any is equivalent to a logical OR and All is equivalent to a logical AND.
5. Select the Identifier you will use for the Value field.
6. Select the operator for the rule.
7. Click Add Condition to add more criteria for the rule. Otherwise proceed to step 8.

8. Select the permissions for the rule. See Device Control permissions for descriptions of each permission.
9. Select whether notifications should be displayed on the endpoint when a Device Control rule is triggered.

IMPORTANT! For Secure Endpoint Windows connector 8.1.3 Engine Notifications under Client User Interface must be enabled in the policy for notifications to be displayed on the endpoint. This is not required for version 8.1.5 and later.

10. Click Save.

Device Control permissions

Permissions control how the connector allows the endpoint to interact with an attached USB mass storage device.

Permission	Description
Block	Do not allow the endpoint to access the device in any way.
Read Only	Only allow the endpoint to read files from the device. Note that users can still manually copy a file from the device onto the endpoint and write to or execute it.
Read and Write Only	Allow the endpoint to read and write files on the device. Note that users can still manually copy a file from the device onto the endpoint and execute it.
Read, Write, and Execute	Allow the endpoint full access to the device. Not available for WPD because this version does not currently support execute.

Add a Configuration to a Policy

A configuration must be assigned to a policy for it to be processed by your endpoints. You can add the configuration to a policy in one of two ways.

1. Go to Management -> Policies. Edit the desired policy and navigate to the Device Control tab. Select the configuration from the pulldown and save the policy.
2. From the Device Management page select the configuration you want to add to a policy. Click Assign to Policies and select one or more policies to assign the configuration to.

IMPORTANT! You can assign multiple configurations to a policy, but only one per configuration type.

Known Issues and Limitations

- Device Control is currently limited to USB mass storage devices and Windows Portable Devices connected via USB.
- Device Control may require reboots when upgrading/uninstalling the connector under certain conditions. If Device Control has been enabled on the endpoint at least once, this will install the Device Control driver on the endpoint and one or more of the following scenarios occurs:
  - (Upgrades) When there are pre-existing external devices while upgrading to version 8.2.1, you may need to reboot for WPD support to work as expected.
  - (Uninstalling) When the driver cannot cleanly detach from external devices that are currently connected to the endpoint.
- USB mass storage devices that are currently attached to the endpoint when the Device Control feature is enabled may not be able to be managed until the devices are re-attached or the endpoint is rebooted.
- If a USB mass storage device is already connected to an endpoint and a new rule is deployed that affects that device (for example, adding a rule to block write access), the actions may appear to be allowed on the device (creating a new file on the device), but when the device is unplugged and re-plugged, then the user will see that the actions were never finalized.
- Sometimes subsequent insertion events might be skipped because of the throttling limit.
- If a USB mass storage device is already connected to an endpoint that was blocked with write permission, and a new rule is deployed that will allow the write permission to the device or the Device Control feature is disabled in the policy, then the write permission will still be blocked if the USB device has NTFS file system, until the device is re-attached.
- Some Android devices connected to an endpoint running version 8.1.7 may disappear from the Windows device manager after upgrading to version 8.2.1. The Device Control rules that were created for this device might not work as expected. To resolve this issue, the device needs to be unplugged and plugged in again.
- The Device Control feature sometimes has limitations working with HyperV virtual machines.
- External applications like iTunes will still be able to manage the devices that are blocked via Device Control rules.

Chapter 4
Exclusions

An exclusion set is a list of directories, file extensions, or threat names that you do not want the Secure Endpoint connector to scan or convict. Go to **Management > Exclusions** to view a list of the exclusion sets. 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 - Allowed Applications to stop the Secure Endpoint connector from quarantining a single file (for example, a false positive detection).

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.

See Best practices for Secure Endpoint Exclusions for further information on creating exclusions.

Configuring Compatibility for Antivirus Products

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

See Antivirus Compatibility Using Exclusions for further details.

Custom Exclusions

Click the **Custom Exclusions** button to view or edit the exclusion sets created by your organization or to create new ones. Each row displays the operating system, exclusion set name, the number of exclusions, the number of groups using the exclusion set, and the number of computers using the exclusion set. You can use the search bar to find exclusion sets by name, path, extension, threat name, or SHA-256. You can also filter the list by operating system by clicking on the respective tabs. Click **View All Changes** to see a filtered list of the Audit Log showing all exclusion set changes.

Click any exclusion set to expand its details. You can click **View Changes** in this view to see changes made to just that particular set.

IMPORTANT! You may not be able to see certain groups or policies depending on the permissions you have to them.

You can also choose to edit or delete the exclusion set from here.

IMPORTANT! You can only delete exclusion sets that are not in use by a policy. The Delete button will be greyed-out (disabled) if the exclusion set is in use by at least one policy.

To create a custom exclusion set, click **New Exclusion Set**. This will display a dialog from which you can select whether the exclusions will be for Secure Endpoint Windows, Secure Endpoint Mac, or Secure Endpoint Linux connectors. Click **Create**.

The new exclusion set is pre-filled with default exclusions. Enter the name for the new exclusion set in the provided field.

Select the exclusion type you would like to add by clicking the empty drop-down menu. (See Exclusion Types)

After selecting the exclusion type, enter the path, threat name, file extension, process, or wild cards for file names, extensions, or paths. Click Add Exclusion if you want to add more exclusions to the set, or if you are finished, click **Save**. Click Revert Changes any time you want to revert to the last saved version of the exclusion set.

You can also quickly add multiple exclusions at a time by clicking Add Multiple Exclusions... You can then enter or paste a list of exclusions into the following dialog, then click Add Exclusions when you are done. Exclusion types will be automatically detected when possible and added to the exclusion set. Any exclusions that aren't detected will be added to the set with a blank exclusion type. For these, you must manually select the exclusion type from the drop-down menu.

IMPORTANT! You can use wild cards when adding multiple exclusions.

After saving, the exclusion set is displayed for review. From here, you can click Edit to make further changes to the set, click View Changes to review the changes made to the exclusion set, or click Delete to remove the set. You can also click to navigate to any of the groups or policies that are assigned to the exclusion set.

Exclusion Types

You can create exclusions based on a threat name, the path to a file, by file extension, by process, or by executable name. Wildcard exclusions are path or file extension exclusions that allow you to use wildcard characters as part of the exclusion.

Threat Exclusions

Threat exclusions let you exclude a particular threat name from being quarantined. 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 be detected and quarantined or generate an event.

Path Exclusions

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.

If some computers in your organization have the Program Files directory on a different drive or path, you can use a KNOWNFOLDERID instead. The above exclusion path would instead be:

```
FOLDERID_ProgramFiles\MyAntivirusAppDirectory
```

IMPORTANT! Path exclusions will prevent the Secure Endpoint connector from scanning all files and subdirectories in the directory specified.

It is strongly recommended that you use the KNOWNFOLDERID (https://learn.microsoft.com/en-us/windows/win32/shell/knownfolderid) if you add an

exclusion by path on Windows. These are variables on Windows computers in case the path is not the same on every system.

IMPORTANT! KNOWNFOLDERID is supported in Secure Endpoint Windows connector 8.1.7 and later. Earlier versions of the connector use CSIDL ((http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx) values. Version 8.1.7 will recognize CSIDL exclusions but earlier connector versions will not recognize KNOWNFOLDERID exclusions.

IMPORTANT! The KNOWNFOLDERID values are case sensitive. For example, you must use FOLDERID_ProgramFiles and not FolderID_programfiles.

File Extension Exclusions

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
```

Wildcard Exclusions

Wildcard exclusions are the same as path or extension exclusions except that you can use an asterisk character as a wild card within the path (including CSIDL paths) or extension. 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/
```

You can also choose **Apply to all drive letters** for Windows wildcard exclusions. This will apply the exclusion to all mounted drives.

Windows Process Exclusions

Process exclusions for the Secure Endpoint Windows connector allow you to exclude running processes from normal File Scans (Secure Endpoint Windows connector version 5.1.1 and later), System Process Protection, Malicious Activity Protection, or Behavioral Protection.

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 KNOWNFOLDERID (https://learn.microsoft.com/en-us/windows/win32/shell/knownfolderid) value for system context folders. 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! KNOWNFOLDERID is supported in Secure Endpoint Windows connector 8.1.7 and later. Earlier versions of the connector use CSIDL ((http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx) values. Version 8.1.7 will recognize CSIDL exclusions but earlier connector versions will not recognize KNOWNFOLDERID exclusions.

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.

For connector versions 7.5.3 and later you can exclude processes by specifying Wildcard Exclusions for the process executable path. The wildcard can be used to represent any number of characters in a single directory. You should only use the wildcard to cover the minimum number of characters required to provide the needed exclusion. The wildcard can also be used alongside characters within a directory to narrow down the exclusion even further.

You can also use a double wildcard to exclude subfolders in a path. This can only be used at the end of a process exclusion.

The following wildcards are supported:

- * character in a path will match only to the next specified character.
- * character at the end of a path will match to the next specified character but not in subdirectories.
- ** at the end of a path will match all subdirectories. You cannot use ** in the middle of a path.

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 along with any network traffic from the application. 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. However, if you do not want any child processes to be scanned or appear in Device Trajectory along with their network traffic, you can fill the checkbox Apply for **child processes**.

Executable Exclusions for Exploit Prevention

Executable exclusions only apply to connectors with Exploit Prevention enabled. An executable exclusion is used to exclude certain executables from being protected by exploit prevention. You should only exclude an executable from exploit prevention if you are experiencing problems or performance issues to maintain a better security posture.

You can check the list of Protected Processes and exclude any from protection by specifying its executable name in the application exclusion field. Executable

exclusions must match the executable name exactly in the format `name.exe`. Wildcards are not supported.

IMPORTANT! Any executables you exclude from exploit prevention will need to be restarted after the exclusion is applied to the connector.

IOC Exclusions

IOC exclusions allow you to exclude Cloud Indications of Compromise. This can be useful if you have a custom or internal application that may not be signed and causes certain IOCs to trigger frequently.

Select IOC from the exclusion type pulldown then select the name of the IOC you would like to exclude. You can also search the list by partial strings.

IMPORTANT! If you exclude a high or critical severity IOC you will lose visibility into it and could leave your organization at risk. You should only exclude these IOCs if you experience a large number of false-positive detections for it.

Linux and Mac Process Exclusions

Process exclusions for the Secure Endpoint Linux and Secure Endpoint Mac connectors allow you to exclude running processes from normal File Scans and Behavioral Protection (Secure Endpoint Linux connector 1.22.0 and later).

You can exclude processes by specifying the full (absolute) path to the process executable and the user name of the process. If you specify both the path and the user for a process exclusion, then both conditions must be met for the process to be excluded. If you leave the user field blank then the exclusion will apply to any process running the specified program.

For connector versions 1.15.2 and later you can exclude processes by specifying Wildcard Exclusions for the process executable path. The wildcard can be used to represent any number of characters in a single directory. For example, if you wanted to exclude all versions of Java from being scanned you could enter this path exclusion:

```
/Library/Java/JavaVirtualMachines/*/Contents/Home/bin/java
```

You should only use the wildcard to cover the minimum number of characters required to provide the needed exclusion. The wildcard can also be used alongside characters within a directory to narrow down the exclusion even further. For example, if you wanted to exclude only a certain version of java from being scanned you could enter this path exclusion:

```
/Library/Java/JavaVirtualMachines/jdk1.7.*.jdk/Contents/Home/bin/
java
```

Child processes created by an excluded process are not excluded by default. For example, if you created a process exclusion for Java, by default any additional processes created by Java would still be scanned and appear in the Device Trajectory along with any network traffic generated from the processes. This could be useful if you don't want to see every time Java runs in the Trajectory, but you want to see if a malicious Java app launches another application like a shell. However, if you do not

want any child processes to be scanned or appear in Device Trajectory along with their network traffic, you can fill the checkbox Apply for **child processes**.

See Process Exclusions in macOS and Linux for more information.

Cisco-Maintained Exclusions

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the Secure Endpoint connector and antivirus, security, or other software. Click the **Cisco-Maintained Exclusions** button to view the list of exclusions. These cannot be deleted or modified and are presented so you can see which files and directories are being excluded for each application. These exclusions may also be updated over time with improvements and new exclusions may be added for new versions of an application. When one of these exclusions is updated, any policies using the exclusion will also be updated so the new exclusions are pushed to your connectors.

Each row displays the operating system, exclusion set name, the number of exclusions, the number of groups using the exclusion set, and the number of computers using the exclusion set. You can use the search bar to find exclusion sets by name, path, extension, threat name, or SHA-256. You can also filter the list by operating system by clicking on the respective tabs.

Antivirus Compatibility Using Exclusions

To prevent conflicts between the connector and antivirus or other security software, you must create exclusions so that the connector doesn't scan your antivirus directory and your antivirus doesn't scan the connector directory. This can create problems if antivirus signatures contain strings that the connector sees as malicious or issues with quarantined files. You can add appropriate Cisco-Maintained Exclusions to your Policies or create your own Custom Exclusions.

See Best practices for Secure Endpoint Exclusions for further information on creating exclusions.

Creating Exclusions in Antivirus Software

In addition to creating exclusions for antivirus products in the connector, you must also create exclusions for the connector in antivirus products running on your endpoints. Consult your antivirus software documentation for instructions on excluding files, directories, and processes from being scanned.

See the Secure Endpoint Troubleshooting TechNotes for additional instructions on creating exclusions for the connector in various antivirus software.

Secure Endpoint Windows connector

Antivirus products must exclude the following directories and any files, directories, and executable files within them:

- C:\Program Files\Cisco\AMP\

IMPORTANT! This is the default install directory. If you have specified a custom install directory, that directory must be excluded.

For antivirus products that require a full path to the executable file for exclusions, you should exclude all binary files in the `C:\Program Files\Cisco\AMP\[connector version]\` directory.

For example:

- `C:\Program Files\Cisco\AMP\[connector version]\ConnectivityTool.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\creport.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\ipsupporttool.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\iptray.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\sfc.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\uninstall.exe`
- `C:\Program Files\Cisco\AMP\[connector version]\updater.exe`
- `C:\Program Files\Cisco\AMP\clamav\[clam version]\freshclam.exe`
- `C:\Program Files\Cisco\AMP\clamav\[clam version]\freshclamwrap.exe`

Where `[connector version]` is in the most recently installed version number of the connector and `[clam version]` is the most recent version of the ClamAV engine.

It may also be necessary to exclude the connector UI log file:

- `C:\ProgramData\Cisco\AMP\IPTray.log`

Secure Endpoint Mac connector

Antivirus products must exclude the following directories and any files, directories, and executable files within them to be compatible with the Secure Endpoint Mac connector:

- `/Library/Application Support/Cisco/AMP for Endpoints Connector`
- `/opt/cisco/amp`

Secure Endpoint Linux connector

Antivirus products must exclude the following directories and any files, directories, and executable files within them to be compatible with the Secure Endpoint Linux connector:

- `/opt/cisco/amp`

If your antivirus product requires a full path to executable files, you should exclude all binary files in `/opt/cisco/amp/bin/` including:

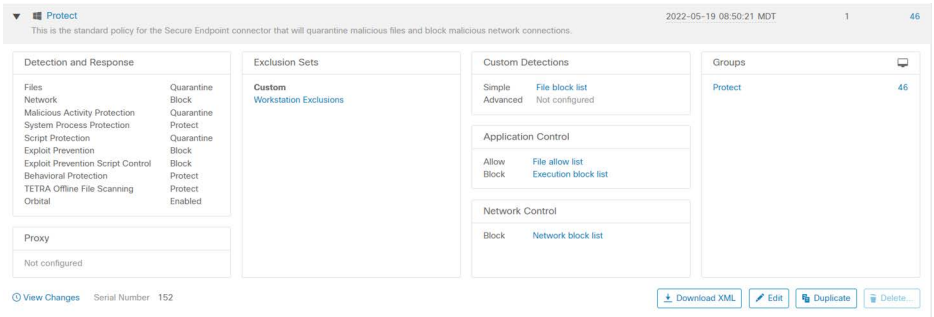
- `/opt/cisco/amp/bin/ampdaemon`
- `/opt/cisco/amp/bin/ampupdater`
- `/opt/cisco/amp/bin/ampscansvc` (version 1.9.0 and later)
- `/opt/cisco/amp/bin/ampcli`
- `/opt/cisco/amp/bin/ampmon`
- `/opt/cisco/amp/bin/ampsupport`
- `/opt/cisco/amp/bin/ampsigncheck`

CHAPTER 5
POLICIES

Outbreak Control and Exclusions sets 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.

Policy Summary

Click on the arrow next to a policy name to toggle between its expanded settings and collapsed view or use the Expand and Collapse All buttons ⊟ ⊞ at the top right of the list to do the same for all the policies on the page.



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.

Click **Edit** or the policy name to modify an existing policy or click **Duplicate** if you want to create a new policy with the same settings.

You can also download the XML file, which contains the specific policy for the connector using the **Download XML** button. The connector installer contains the policy by default and this should only be used in specific troubleshooting scenarios.

IMPORTANT! Duplicate exclusions will be removed in the downloaded XML file.

Click **New Policy...** to create a new policy. Next, choose whether you want to create a policy for:

- Secure Endpoint Windows
- Secure Endpoint Android
- Secure Endpoint Mac
- Secure Endpoint Linux
- Secure Endpoint iOS

Secure Endpoint Windows Connector Policy

This section describes the policy options that are available for Secure Endpoint Windows connectors.

Windows Connector: Required Policy Settings

Clicking New Policy will take you to the first of a series of configuration pages that you must complete before you can save your new policy. Fill in the settings and click Next to advance through the pages. The settings on these pages are described below.

IMPORTANT! You cannot access the Outbreak Control, Product Updates, and Advanced Settings pages for the new policy before completing these configuration pages.

Name and Description

The Name box enables you to create a name that you can use to recognize the policy. You can add more details about the policy in the optional description box.

Modes and Engines

This page contains settings pertaining to conviction modes and detection engines. See Windows Connector Support Tools for more information on each engine. Click **Apply Workstation Settings** or **Apply Server Settings** to quickly set all the conviction modes in the policy to the recommended settings for workstations or servers.

Conviction Modes

Conviction Modes specify how the connector responds to suspicious files, network activity, and processes. Setting Files to Audit will stop the Secure Endpoint connector

from quarantining any files. This setting only applies to version 3.1.0 and higher of the Secure Endpoint connector.

IMPORTANT! 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.

The Malicious Activity Protection (or MAP) engine defends your endpoints from ransomware attacks by identifying malicious actions of processes when they execute and stops them from encrypting your data. Audit logs the event but will not take action on the detected process. Quarantine mode quarantines the detected process, and Block stops the process from executing. You can also set the engine to Monitor Network Drives.

System Process Protection protects critical Windows system processes from being compromised through memory injection attacks by other processes. Protect blocks attacks on critical Windows system processes.

Script Protection will block malicious script files from executing when in **Quarantine** mode. **Audit** mode will create an event when a malicious script is executed but will not prevent it from executing.

The Exploit Prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. **Audit** mode is available in connector version 7.3.1 and later. Earlier versions of the connector will treat Audit mode the same as Block mode.

IMPORTANT! If you disable Exploit Prevention you will have to restart any of the protected processes. See Protected Processes for the list of protected processes.

Script Control prevents certain DLLs from being loaded by some applications and their child processes. In **Block** mode, the engine will kill a process if it or one of its child processes attempts to load certain DLLs. **Audit** mode will create events when the activity is detected but won't kill any processes.

Behavioral Protection helps prevent malicious activity that matches a set of behavioral signatures by alerting on activity, quarantining files, and ending processes in **Protect** mode. **Audit** mode will create events when matching activity is detected but will not take any actions.

Detection Engines

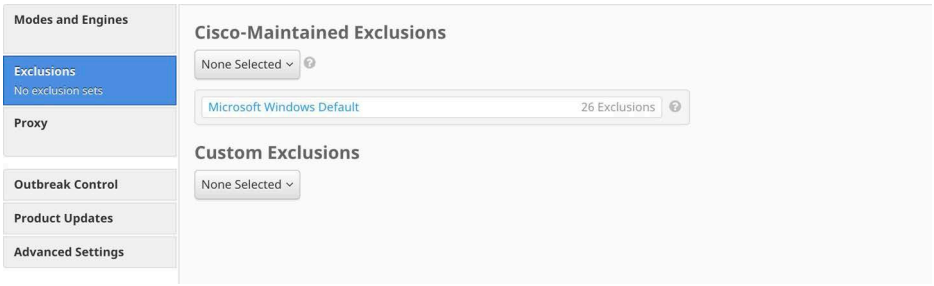
You can enable additional detection engines to protect the endpoint from malware without connecting to the Cisco Cloud to query each file.

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. More TETRA settings are available in **Advanced Settings >** TETRA.

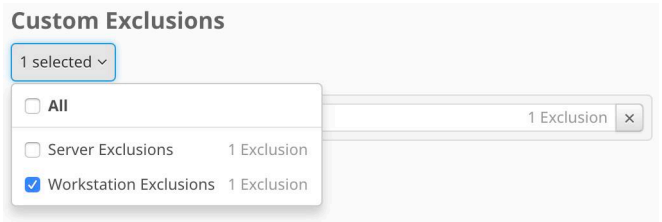
Exclusions

You can select exclusion sets to apply to the policy here. All new Windows policies include Cisco-Maintained Exclusions for certain components of the Windows

operating system. This set of exclusions cannot be removed. You can choose other Cisco-Maintained Exclusions to add to the policy depending on the applications present in the policy group and add your Custom Exclusions to the policy.

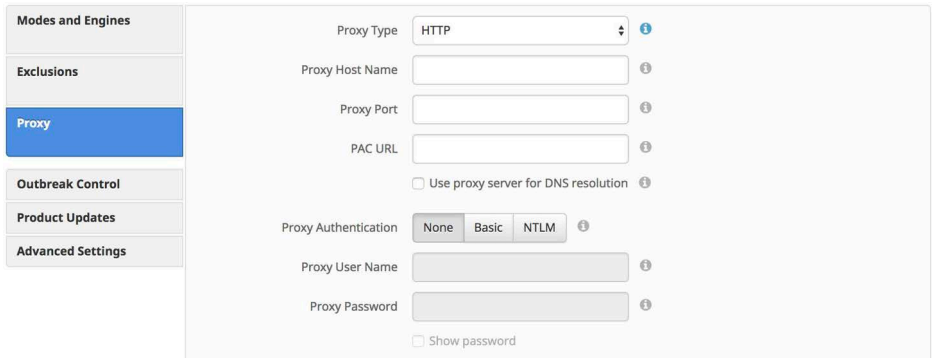


Click the drop-down menu for either the Cisco-maintained exclusions or your custom exclusions and fill the checkboxes to select exclusion sets. See Exclusions for more information.



Proxy

Complete your proxy configuration on this page.



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

Proxy Host Name is the name or the IP address of the proxy server. Only IPv4 addresses are supported.

Proxy Port is the port the proxy server runs on.

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 (Windows only) lets you specify whether all connector DNS queries should be performed on the proxy server.

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.

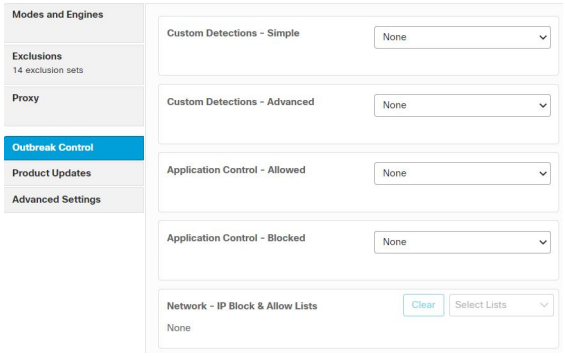
IMPORTANT! If NTLM is selected as the proxy authentication type, this field must be in domain\username format.

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

Windows Connector: Other Policy Settings

Once you have filled out the required configuration pages, you will be able to access pages for Outbreak Control, Product Updates, and Advanced Settings. The following sections will describe the settings.

Outbreak Control



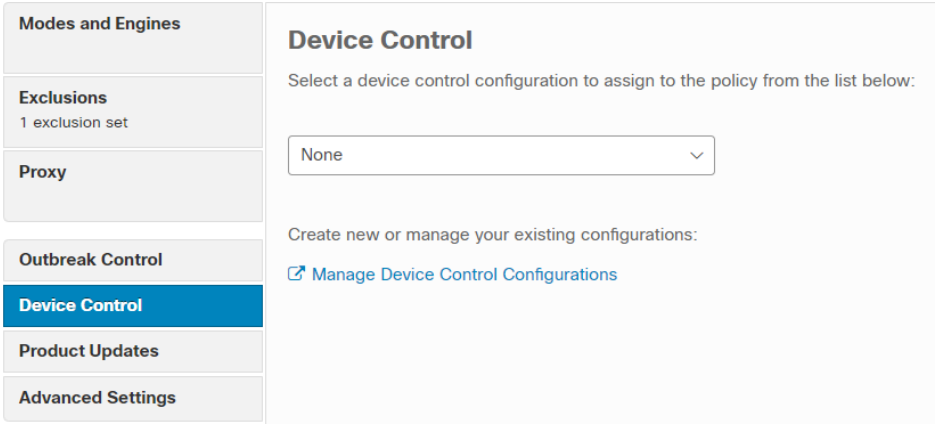
On this page, select the lists you want to assign to the policy. See Custom Detections - Simple, Custom Detections - Advanced, Application Control - Allowed Applications,

Application Control - Blocked Applications, and Network - IP Block & Allow Lists for details on creating these lists. Note that not all connectors support all list types.

IMPORTANT! Network - IP Blocked & Allowed Lists will only work if you enable Device Flow Correlation in the Network tab in Advanced Settings.

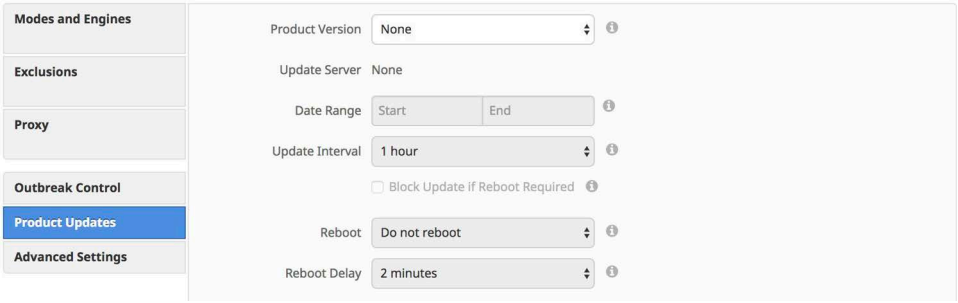
If there are IP allowed or blocked lists available, you can click Select Lists to choose the ones you want to add to the policy. Fill the checkboxes of all the lists you want to add from the drop-down menu. You can add multiple IP lists to a single policy; however, IP allowed list entries will override IP blocked list entries.

Windows Connector: Device Control



Add any Device Control configurations to your policy. Select the configuration from the pulldown to add it. You can only add one configuration per policy.

Windows Connector: 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** drop-down menu 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. There will be an option to update Orbital only if you have enabled Orbital and selected With Connector under the Update Schedule.

You can then define the window in which updates are allowed to occur by choosing a Date Range. In Date Range, click Start to select a date and time for your start window and End to select a date and time for your end window. You can also select This Month to set the date range from the current day to the end of the current month, Next 7 Days to set the range to the next 7 days, or Next 30 Days to set the range to the next 30 days. The **Update Interval** allows you to specify how long your connectors will wait between checks for new product updates, including Orbital updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic.

Between the times set in the Date Range, 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.

If you are updating to version 4.3 or later of the Secure Endpoint Windows connector you will be presented with 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. See this article for specific update reboot requirements.

IMPORTANT! Starting with Secure Endpoint Windows connector 7.x.x, upgrading the connector from 7.x.x to any newer version should no longer require a reboot to complete. While most upgrades will not require a reboot, there may be occasional instances where a reboot is still required. For a list of circumstances that require a reboot, see Secure Endpoint Windows Connector Update Reboot Requirements.

Reboot presents the options **Do not reboot**, **Ask for reboot** from the user, or **Force reboot after...**, which allows you to choose a **Reboot Delay.**

IMPORTANT! If an update displays “Reboot required”, the connector service will be stopped until the computer is rebooted. To avoid leaving computers vulnerable after such updates, check Block Update if Reboot Required.
If an update displays “Reboot suggested”, the connector service will continue to run after the update, but any new functionality from the update will not be available until the computer is rebooted
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.

Windows Connector: Advanced Settings

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 Secure Endpoint 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.

Enable Connector Protection allows you to require a password to uninstall the connector or stop its service.

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.

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

IMPORTANT! If you include any special characters in the password, you must escape the characters when entering the password in a command prompt or PowerShell on the endpoint.

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

Command Line Capture (Secure Endpoint Windows connector 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 Secure Endpoint. This information will be displayed in Device Trajectory for administrators as long as they have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication enabled.

IMPORTANT! Command Line Capture may truncate exceptionally long command line arguments. Contact Support if this is an issue.

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.

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 connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud.

Engine Notifications display notifications generated by the different connector engines. These include:

- Cloud lookups
- TETRA
- Malicious Activity Protection
- System Process Protection
- Exploit Prevention
- Device Flow Correlation
- Endpoint IOC cataloging

Hide Exclusions suppresses the display of configured exclusions from the connector user interface. (Available on Secure Endpoint Windows connector versions 5.1.3 and higher)

Allow User to Update TETRA Definitions enables a button on the Secure Endpoint Windows connector UI to update TETRA definitions on demand. (Available for Secure Endpoint Windows connector versions 7.2.11 and higher)

File and Process Scan

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.

Verbose History (Windows connector 5.1.9 or higher only) controls whether or not Secure Endpoint Windows connectors will write verbose history information to the history.db file.

On Execute Mode can run in two different modes: **Active** or **Passive**. In Active mode, files and scripts are blocked from being executed until a determination of whether or not it is malicious or a timeout is reached. In Passive mode, files and scripts are 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 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 connector. Any archive file larger than the threshold set will not be scanned.

Cache

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 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 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 1 week.

Unknown Cache TTL is the time 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 for which a file that is in an Application Control - Blocked Applications 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.

Endpoint Isolation

Endpoint Isolation lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation.

Allow DNS allows the endpoint to perform DNS lookups while it is isolated. The connector will automatically add the address of the DNS server configured in the endpoint's network settings to the allow list. You will need to add the addresses of your DNS servers to the allow list manually if you turn this setting off.

Allow DHCP allows the endpoint to send and receive traffic on UDP ports 67 and 68 so it can obtain or renew a DHCP lease. You can safely turn this off if you use static IP addresses. You will need to add the addresses of your DHCP servers to the allow list manually if you turn this setting off.

Allow use with proxy is provided for advanced users with specific proxy configuration needs. This feature is useful if you have a proxy to manage internal/secure communication that is distinct from a more generic internet proxy. However, if you

choose to use a proxy you must ensure the Secure Endpoint Cloud infrastructure is allowed to send and receive traffic through that proxy on connector versions before 7.5.1.

IMPORTANT! An isolated endpoint with Allow use with proxy turned on can still send and receive network traffic through the proxy if the proxy is in the IP isolation allow list. In most cases this negates the effects of isolation and leaves the endpoint exposed. If the proxy is not specified on your IP isolation allow list, the endpoint cannot communicate with the Secure Endpoint Cloud on connector versions before 7.5.1, in which case you can only Stop a Windows Isolation Session From the Command Line on the endpoint. Connector versions 7.5.1 and later retain the ability to communicate with the Cisco cloud from behind the proxy when isolated. We recommend careful network testing before rolling out isolation with a proxy enabled.

You can specify the **IP Allow Lists** the connector will use during an isolation session. Use the Select Lists pulldown to specify the IP Isolation Allow Lists to use with this policy.

Orbital

IMPORTANT! Orbital is available for customers with Secure Endpoint advantage package or higher.

Orbital allows you to query endpoints for detailed information wherever you have Orbital deployed. For details on using Orbital, see the Orbital documentation at https://orbital.amp.cisco.com/help/.

To enable Orbital in a policy, select the **Enable Orbital Advanced Search** checkbox, then click **Save**.

Orbital will be installed on any computers running Windows 10 1709 or later and Windows Server 2012, 2012 R2, 2016 and later that have not previously had the feature enabled. The connector will send an event to the Secure Endpoint console once the installation has completed successfully. The install interval for Orbital is the same as the Update Interval setting under Windows Connector: Product Updates (default value:1 hour).

The **Update Schedule** allows you to define if Orbital will be updated automatically whenever a new version is available or scheduled under Windows Connector: Product Updates.

You can force an Orbital update in connector version 7.4.5 and higher using the following command from the connector install directory using an account with administrator permission:

```
sfc.exe -forceOrbitalUpdate
```

This command will remove any cached versions that failed and retry the current version.

IMPORTANT! Orbital cannot be enabled while an endpoint is isolated.

IMPORTANT! If you disable Orbital for a policy, it will disable the service but it will not uninstall Orbital from your endpoints. Enabling it again will restart the service.

Engines

Monitor Network Drives allows you to set the Malicious Activity Protection engine to detect malicious activity from the local computer affecting network drives. Note that this setting may cause slowness when monitoring network drives over a VPN. Consider putting users who regularly access network drives over a VPN into a group that uses a policy with this setting disabled. This setting only applies to Secure Endpoint Windows connector version 6.3.1 and later.

IMPORTANT! If the Malicious Activity Protection engine detects activity on a network drive it will be able to block and quarantine the local process but it will not quarantine the file from the network drive.

Script Control sets the Script Protection behavior. Default ties the Script Control setting to the same setting as Exploit Prevention under the Modes and Engines tab. You can use the block, audit, and disabled settings to keep Script Control behavior separate from the Exploit Prevention behavior.

IMPORTANT! Exploit Prevention must be enabled to use this feature. These settings only apply to Secure Endpoint Windows connector 7.3.5 and later. Earlier versions will use the same setting as Exploit Prevention.

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.

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.

ETHOS can be resource intensive so it is limited to scanning files up to 5MB on version 6.2.1 and higher of the Secure Endpoint Windows connector. 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.

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.

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.

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.

Enable Event Tracing for Windows will improve the detection of malicious activity on your endpoints when Behavioral Protection is enabled. When the setting is active your Secure Endpoint Windows connectors will make the following changes to the Windows Audit Policy on each endpoint:

- Audit User Account Management Success - enabled
- Audit Logon Success - enabled
- Audit Logon Failure - enabled
- Audit Security System Extension Success - enabled
- Audit Other Object Access Events Success - enabled

The connector will enforce these settings on every Heartbeat Interval to ensure continued monitoring.

This setting only applies to Secure Endpoint Windows connector 7.3.5 and later running on Windows 10 or Windows Server 2019 and later.

IMPORTANT! The Windows Audit Policy settings need to be reset on each endpoint if you disable event tracing.

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 in this tab or in the Modes and Engines tab.

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.

Deep Scan Files determines whether the connector scans the contents of product install and CHM files.

Detect Expanded Threat Types detects archive bombs and applications that could be used maliciously.

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. You can view the version of TETRA definitions and update status for a computer from the Computer Management page.

Local Secure Endpoint Update Server should only be enabled if you have set up a Secure Endpoint Update Server for your connectors to retrieve TETRA definitions. Click the **Secure Endpoint Update Server Configuration** link to download the server. It may take an hour or longer for the Secure Endpoint Update Server to download initial content from the Cisco Cloud.

IMPORTANT! Only Secure Endpoint Windows connector 5.1.13 and later can use a local Secure Endpoint Update Server.

The **Secure Endpoint Update Server** setting has to specify the host name or IP address of the local Secure Endpoint Update Server. Do not include HTTP:// or HTTPS:// in this field.

Use HTTPS for TETRA Definition Updates requires a local Secure Endpoint Update Server. The Secure Endpoint Update Server running in self-hosted mode can only support the HTTP protocol on port 80. If the HTTPS protocol is desired, an HTTPS-enabled Web server, such as Apache, or Nginx has to be utilized, along with valid SSL certificates.

Network

The Network tab contains settings to for the network flow capabilities of your connectors, such as device flow correlation settings.

Enable Device Flow Correlation 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. This option is only available if you have selected Blocking as the detection action.

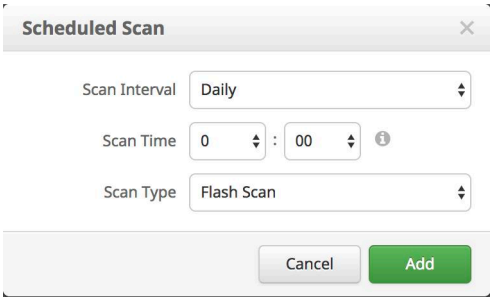
WARNING! Before enabling this feature, make sure you have added any applications allowed in your environment to an allowed list, particularly any proprietary or custom software.

Blocked List Data Source enables you to select the IP blocked lists your connectors use. If you select **Custom**, your connectors will only use the IP blocked lists 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 Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos 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 blocked lists you have added to the policy and the Cisco Intelligence Feed.

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 7 days 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 **+New under 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. A **Custom** scan will scan a particular path that you give it.

Identity Persistence

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

Identity Persistence 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 Organization**: New connectors look for the most recent connector that has the same MAC address to synchronize with across all policies in the organization 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 Host name across Organization**: New connectors look for the most recent connector that has the same host name to synchronize with across all policies in the organization that have Identity Synchronization set to a value other than None.
- **By Host name 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 Secure Endpoint console.

Secure Endpoint Mac Connector Policy

This section describes the policy options that are available for Secure Endpoint Mac connectors.

Mac Connector: Required Policy Settings

Clicking New Policy will take you to the first of a series of configuration pages that you must complete before you can save your new policy. Fill in the settings and click Next to advance through the pages. The settings on these pages are described below.

IMPORTANT! You cannot access the Outbreak Control, Product Updates, and Advanced Settings pages for the new policy before completing these configuration pages.

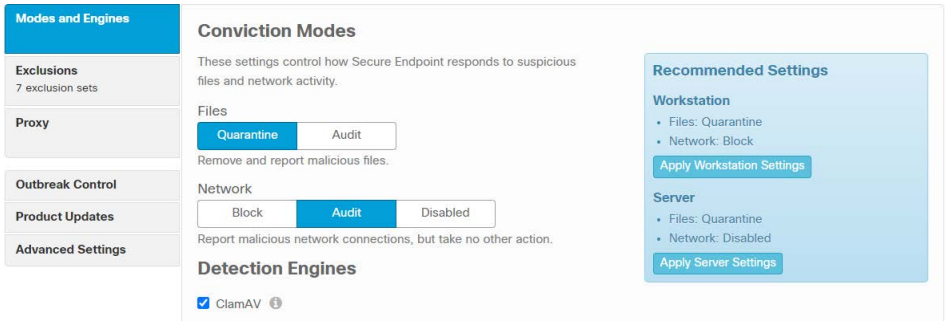
This section describes the policy options that are available for Secure Endpoint Mac connectors.

Name and Description

The Name box enables you to create a name that you can use to recognize the policy. You can add more details about the policy in the optional description box.

Modes and Engines

This page contains settings pertaining to conviction modes and detection engines.



Conviction Modes

Conviction Modes specify how the connector responds to suspicious files and network activity. Setting Files to Audit will stop the Secure Endpoint connector from quarantining any files. This setting only applies to version 3.1.0 and higher of the Secure Endpoint 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.

Detection Engines

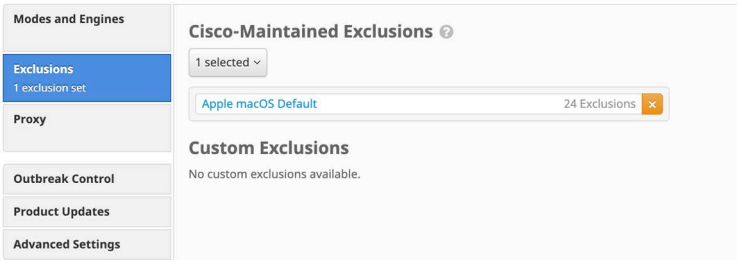
Windows, Mac, and Linux connectors have the option of enabling offline detection engines (TETRA for Windows and ClamAV for Mac and Linux) to protect the endpoint from malware without connecting to the Cisco Cloud to query each file.

ClamAV is a full antivirus replacement and should never be enabled if another antivirus engine is installed. ClamAV can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment. More ClamAV settings are available in Advanced Settings.

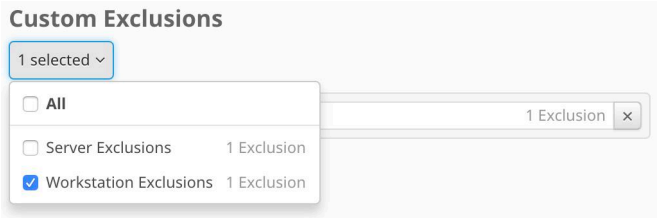
Exclusions

You can select exclusion sets to apply to the policy here. All new Mac policies include Cisco-Maintained Exclusions for certain components of MacOS. This exclusion set cannot be removed. You can choose other Cisco-Maintained Exclusions to add to the

policy depending on the applications present in the policy group and add your Custom Exclusions to the policy.

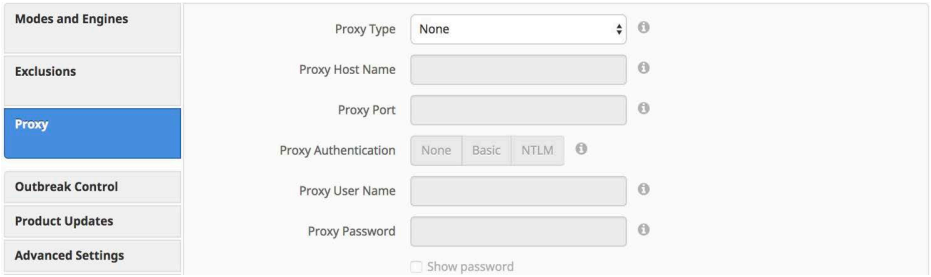


Click the drop-down menu for either the Cisco-maintained exclusions or your custom exclusions and fill the checkboxes to select exclusion sets. See Exclusions for more information.



Proxy

Complete your proxy configuration on this page.



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

IMPORTANT! The mac_system_pac proxy type requires connector version 1.22.0 and later. The connector uses the Automatic Proxy Configuration URL in the macOS network system preferences to configure the proxy. A proxy won't be used unless this URL is specified. See Secure Endpoint Mac Proxy Automatic Configuration (PAC) Setup Guide for more information.

Proxy Host Name is the name or the IP address of the proxy server. Only IPv4 addresses are supported.

Proxy Port is the port the proxy server runs on.

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.

Mac Connector: Other Policy Settings

Once you have filled out the required configuration pages, you will be able to access pages for Outbreak Control, Product Updates, and Advanced Settings. The following sections will describe the settings.

IMPORTANT! The Network policy type is available if Cisco Defense Center is integrated with Secure Endpoint. The Network policy contains some of these settings. For more information on Defense Center integration with Secure Endpoint, see your Defense Center documentation.

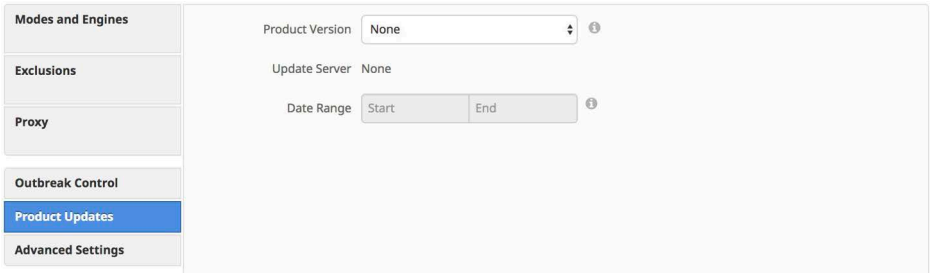
Mac Connector: Outbreak Control

On this page, select the lists you want to assign to the policy. See Custom Detections - Simple, Custom Detections - Advanced, Application Control - Allowed Applications, Application Control - Blocked Applications, and Network - IP Block & Allow Lists for details on creating these lists. Note that not all connectors support all list types.

IMPORTANT! Network - IP Blocked & Allowed Lists will only work if you enable Device Flow Correlation in the Network tab in Advanced Settings.

If there are IP blocked or allowed lists available, you can click Select Lists to choose the ones you want to add to the policy. Fill the checkboxes of all the lists you want to add from the drop-down menu. You can add multiple IP lists to a single policy; however, IP allowed list entries will override IP blocked list entries.

Mac Connector: Product Updates

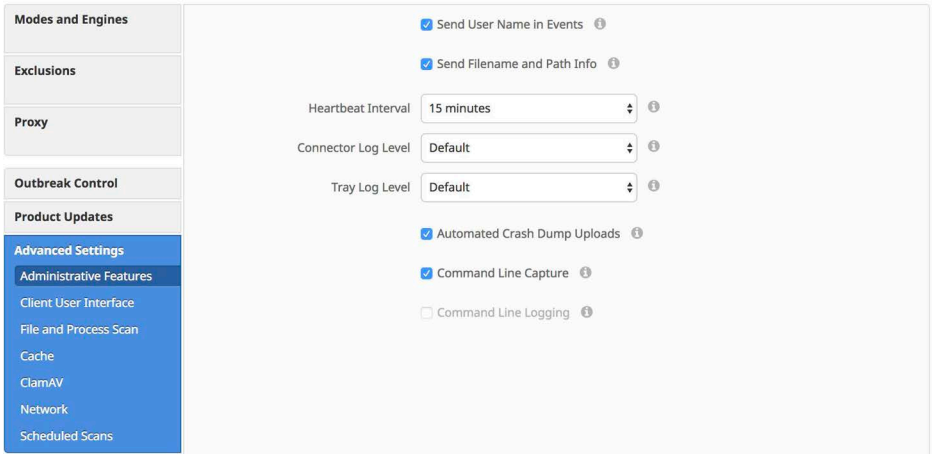


When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** drop-down menu showing which version you are going to and it will populate the **Update Server** so you can see where the files will be pulled from. There will be an option to update Orbital only if you have enabled Orbital and selected With Connector under the Update Schedule.

You can then define the window in which updates are allowed to occur by choosing a Date Range. In Date Range, click Start to select a date and time for your start window and End to select a date and time for your end window. You can also select This Month to set the date range from the current day to the end of the current month, Next 7 Days to set the range to the next 7 days, or Next 30 Days to set the range to the next 30 days. Between the times set in the Date Range, 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.

Mac Connector: Advanced Settings

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 Secure Endpoint 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.

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

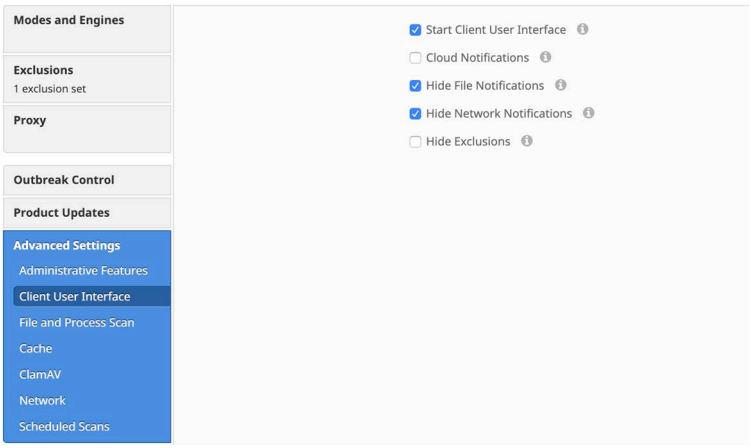
Command Line Capture (Secure Endpoint Mac 1.5.0 and higher) allows the connector to capture command line arguments (including usernames, filenames, passwords, etc.) used during file execution and send the information to Secure Endpoint. This information will be displayed in Device Trajectory for administrators as long as they

have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication enabled.

IMPORTANT! Command Line Capture requires macOS 10.12 or higher to be installed.

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.

Client User Interface



Start Client User Interface allows you to specify whether or not to completely hide the connector user interface.

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

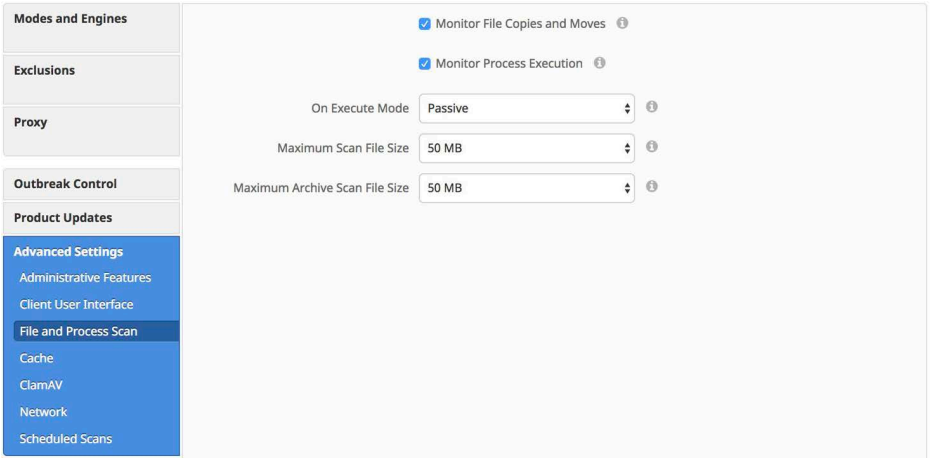
Cloud Notifications are balloon pop-ups that come from the menu bar when the connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud.

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.

Hide Exclusions will suppress the display of configured exclusions from the connector user interface.

File and Process Scan



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.

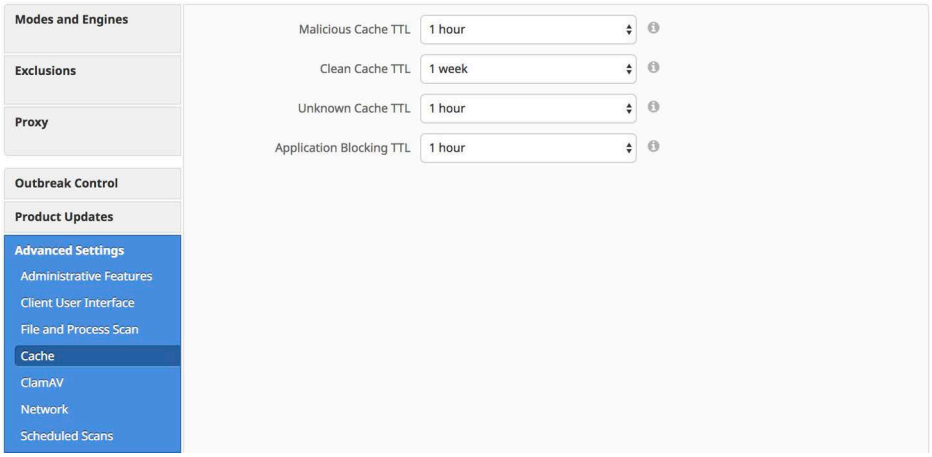
On Execute Mode can run in two different modes: **Active** or **Passive**. In Active mode, the file is blocked from being executed until a determination of whether or not a file is malicious or a timeout is reached. In Passive mode, the file is allowed to be executed and in parallel the file is looked 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 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 connector. Any archive file larger than the threshold set will not be scanned.

Cache



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 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 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 1 week.

Unknown Cache TTL is the time 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 for which a file that is in an Application Control - Blocked Applications 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.

Endpoint Isolation

Endpoint Isolation lets you block incoming and outgoing network activity on a Mac computer to prevent threats such as data exfiltration and malware propagation.

Allow DNS allows the endpoint to perform DNS lookups while it is isolated. The connector will automatically add the address of the DNS server configured in the endpoint's network settings to the allow list. You will need to add the addresses of your DNS servers to the allow list manually if you turn this setting off.

Allow DHCP allows the endpoint to send and receive traffic on UDP ports 67 and 68 so it can obtain or renew a DHCP lease. You can safely turn this off if you use static IP addresses. You will need to add the addresses of your DHCP servers to the allow list manually if you turn this setting off.

You can specify the **IP Allow Lists** the connector will use during an isolation session. Use the Select Lists pulldown to specify the IP Isolation Allow Lists to use with this policy.

Orbital

IMPORTANT! Orbital is available for customers with Secure Endpoint advantage package or higher.

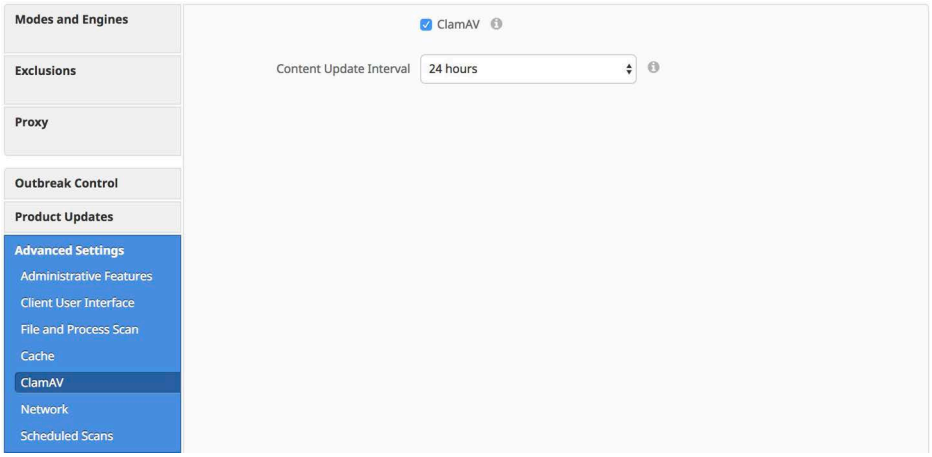
Orbital allows you to query endpoints for detailed information wherever you have Orbital deployed. For details on using Orbital, see the Orbital documentation at https://orbital.amp.cisco.com/help/.

To enable Orbital in a policy, select the **Enable Orbital Advanced Search** checkbox, then click **Save**.

Orbital will be installed on any computers running macOS 10.15 or later with an Intel processor or macOS 12 or later with Apple silicon. Orbital is supported on Apple silicon with Secure Endpoint Mac connector version 1.20 or later, and requires Orbital Node 1.21 or later. The connector will send an event to the Secure Endpoint console once the installation has completed successfully. The **Update Schedule** allows you to define if Orbital will be updated automatically whenever a new version is available or scheduled under Mac Connector: Product Updates.

IMPORTANT! If you disable Orbital for a policy, it will stop and disable the service but it will not uninstall Orbital from your endpoints. Enabling it again will restart the service and re-enable Orbital updates.

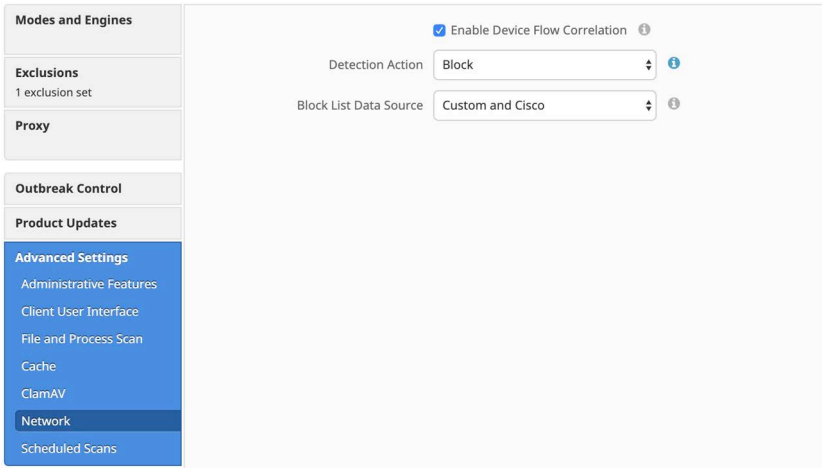
ClamAV



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.

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. You can view the version of ClamAV definitions and update status for a computer from the Computer Management page.

Network



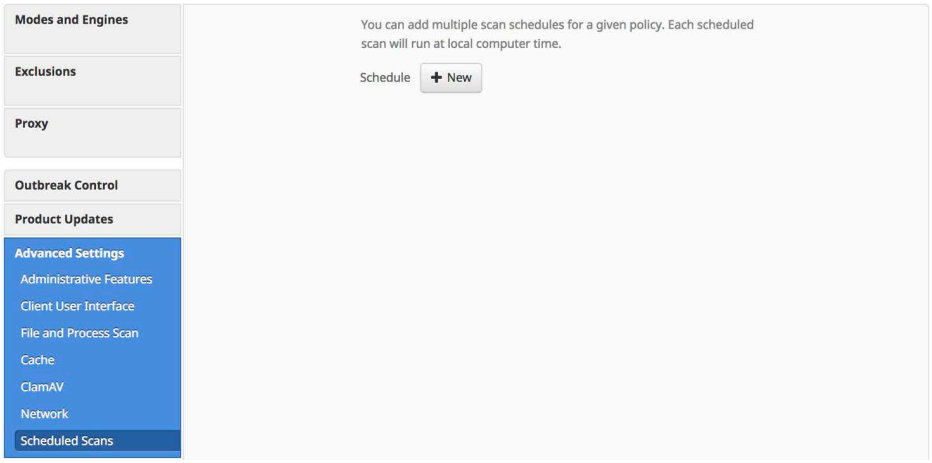
The Network tab contains settings to for the network flow capabilities of your connectors, such as device flow correlation settings.

Enable Device Flow Correlation 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.

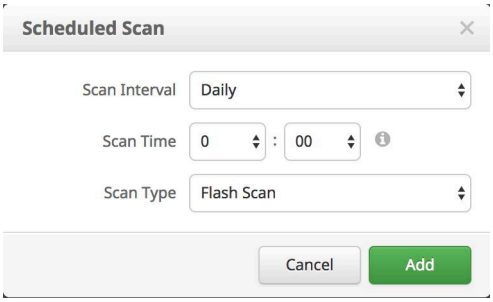
Blocked List Data Source allows you to select the IP blocked lists your connectors use. If you select **Custom**, your connectors will only use the IP blocked lists you have added to the policy. Choose **Cisco** to have your connectors only use the Cisco Intelligence Feed to define malicious sites. The Cisco Intelligence Feed represents IP addresses determined by Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If the Talos 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 blocked lists you have added to the policy and the Cisco Intelligence Feed.

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 7 days 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 **+New under 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. A **Custom** scan will scan a particular path that you give it.

Secure Endpoint Linux Connector Policy

This section describes the policy options that are available for Secure Endpoint Linux connectors.

Linux Connector: Required Policy Settings

Clicking New Policy will take you to the first of a series of configuration pages that you must complete before you can save your new policy. Fill in the settings and click Next to advance through the pages. The settings on these pages are described below.

IMPORTANT! You cannot access the Outbreak Control, Product Updates, and Advanced Settings pages for the new policy before completing these configuration pages.

This section describes the policy options that are available for Secure Endpoint Linux connectors.

Name and Description

The Name box enables you to create a name that you can use to recognize the policy. You can add more details about the policy in the optional description box.

Modes and Engines

This page contains settings pertaining to conviction modes and detection engines.

Conviction Modes

Conviction Modes specify how the connector responds to suspicious files and network activity. Setting Files to Audit will stop the Secure Endpoint connector from quarantining any files. This setting only applies to version 3.1.0 and higher of the Secure Endpoint 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.

Behavioral Protection helps prevent malicious activity that matches a set of behavioral signatures by alerting on activity, quarantining files, and ending processes in **Protect** mode. **Audit** mode will create events when matching activity is detected but will not take any actions.

Detection Engines

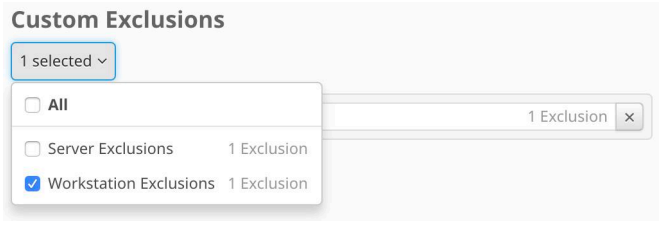
Windows, Mac, and Linux connectors have the option of enabling offline detection engines (TETRA for Windows and ClamAV for Mac and Linux) to protect the endpoint from malware without connecting to the Cisco Cloud to query each file.

ClamAV is a full antivirus replacement and should never be enabled if another antivirus engine is installed. ClamAV can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment. More ClamAV settings are available in Advanced Settings.

Exclusions

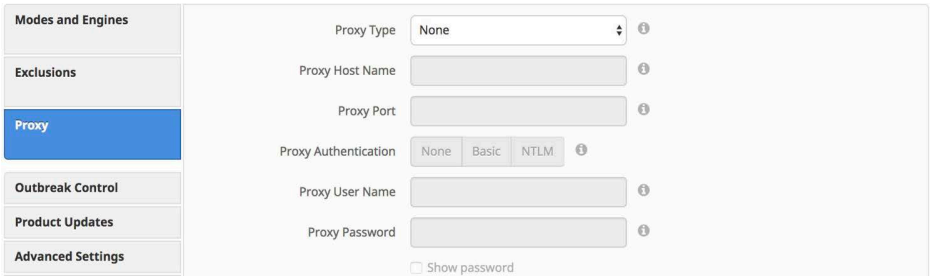
You can select exclusion sets to apply to the policy here.

Click the drop-down menu and fill the checkboxes to select custom exclusion sets. See Exclusions for more information.



Proxy

Complete your proxy configuration on this page.



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

Proxy Host Name is the name or the IP address of the proxy server. Only IPv4 addresses are supported.

Proxy Port is the port the proxy server runs on.

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.

Linux Connector: Other Policy Settings

Once you have filled out the required configuration pages, you will be able to access pages for Outbreak Control, Product Updates, and Advanced Settings. The following sections will describe the settings.

IMPORTANT! The Network policy type is available if Cisco Defense Center is integrated with Secure Endpoint. The Network policy contains some of these settings. For more information on Defense Center integration with Secure Endpoint, see your Defense Center documentation.

Linux Connector: Outbreak Control

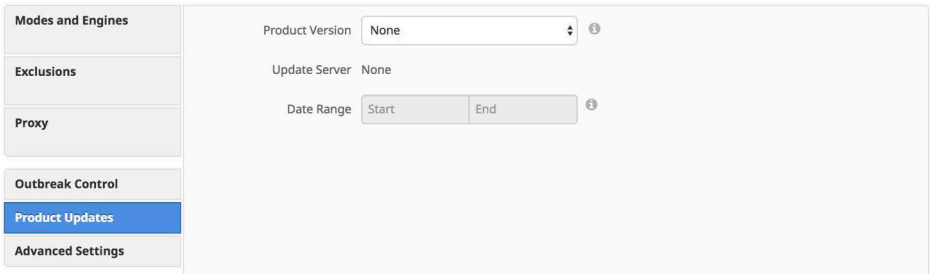
On this page, select the lists you want to assign to the policy. See Custom Detections - Simple, Custom Detections - Advanced, Application Control - Allowed Applications,

Application Control - Blocked Applications, and Network - IP Block & Allow Lists for details on creating these lists. Note that not all connectors support all list types.

IMPORTANT! Network - IP Blocked & Allowed Lists will only work if you enable Device Flow Correlation in the Network tab in Advanced Settings.

If there are IP allowed or blocked lists available, you can click Select Lists to choose the ones you want to add to the policy. Fill the checkboxes of all the lists you want to add from the drop-down menu. You can add multiple IP lists to a single policy; however, IP allowed lists will override IP blocked list entries.

Linux Connector: Product Updates



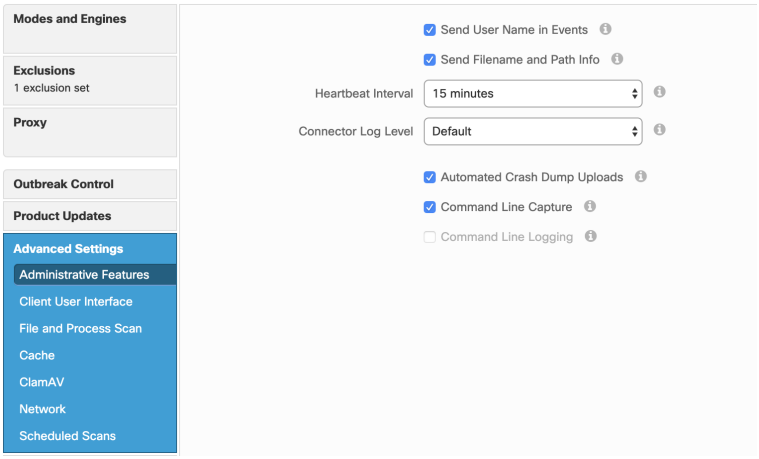
When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** drop-down menu showing which version you are going to and it will populate the **Update Server** so you can see where the files will be pulled from. There will be an option to update Orbital only if you have enabled Orbital and selected With Connector under the Update Schedule. Certain updates will require a reboot to install properly. See this article for specific update reboot requirements.

You can then define the window in which updates are allowed to occur by choosing a Date Range. In Date Range, click Start to select a date and time for your start window and End to select a date and time for your end window. You can also select This Month to set the date range from the current day to the end of the current month, Next 7 Days to set the range to the next 7 days, or Next 30 Days to set the range to the next 30 days.

Between the times set in the Date Range, 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.

Linux Connector: Advanced Settings

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 Secure Endpoint 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.

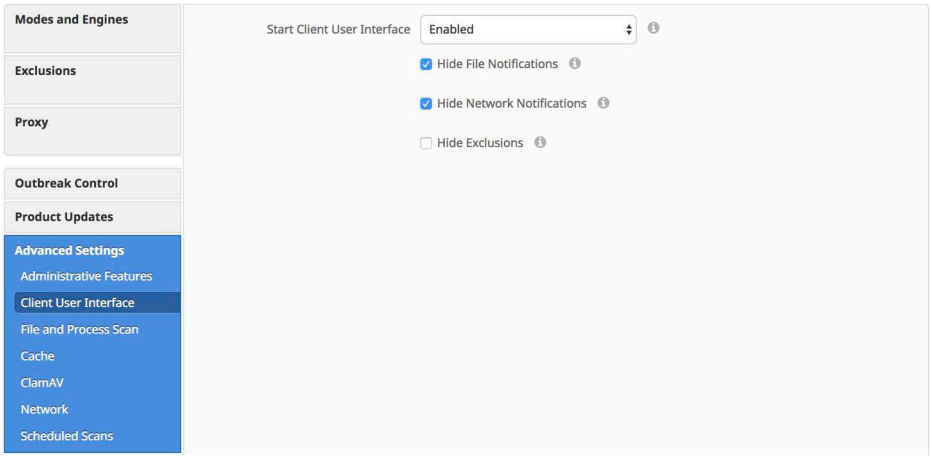
WARNING! When **connector Log Level** is set to Debug, it can cause log files to consume an additional 550MB of drive space.

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

Command Line Capture (Secure Endpoint Linux connector 1.5.0 and higher) allows the connector to capture command line arguments (including usernames, filenames, passwords, etc.) used during file execution and send the information to Secure Endpoint. This information will be displayed in Device Trajectory for administrators as long as they have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication 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.

Client User Interface



Start Client User Interface allows you to specify whether or not to completely hide the connector user interface. Choosing Disabled, the connector runs as a service, but the user interface components will not run. With Command Line Only and Privileged Command Line Only, the connector runs as a service without the interface components, but allows user access via the terminal.

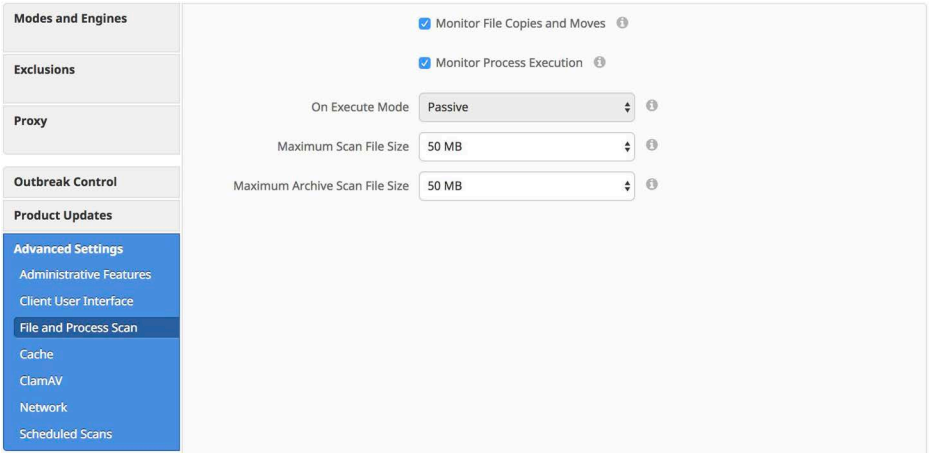
IMPORTANT! If you change this setting, your connectors will have to be restarted before it takes effect.

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.

Hide Exclusions will suppress the display of configured exclusions from the connector user interface.

File and Process Scan



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.

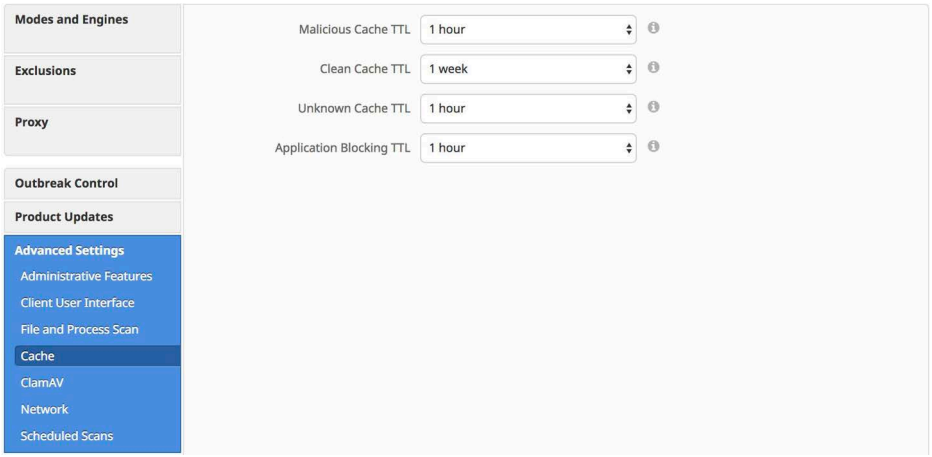
On Execute Mode can run in two different modes: **Active** or **Passive**. In Active mode, the file is blocked from being executed until a determination of whether or not a file is malicious or a timeout is reached. In Passive mode, the file is allowed to be executed and in parallel the file is looked 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 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 connector. Any archive file larger than the threshold set will not be scanned.

Cache



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 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 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 1 week.

Unknown Cache TTL is the time 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 for which a file that is in an Application Control - Blocked Applications 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.

Orbital

IMPORTANT! Orbital is available for customers with Secure Endpoint advantage package or higher.

Orbital allows you to query endpoints for detailed information wherever you have Orbital deployed. For details on using Orbital, see the Orbital documentation at https://orbital.amp.cisco.com/help/.

To enable Orbital in a policy, select the **Enable Orbital Advanced Search** checkbox, then click **Save**.

The connector will send an event to the Secure Endpoint console once the installation has completed successfully. The **Update Schedule** allows you to define if Orbital will be updated automatically whenever a new version is available or scheduled under Linux Connector: Product Updates.

If you disable Orbital for a policy, it will stop and disable the service but it will not uninstall Orbital from your endpoints. Enabling it again will restart the service and re-enable Orbital updates.

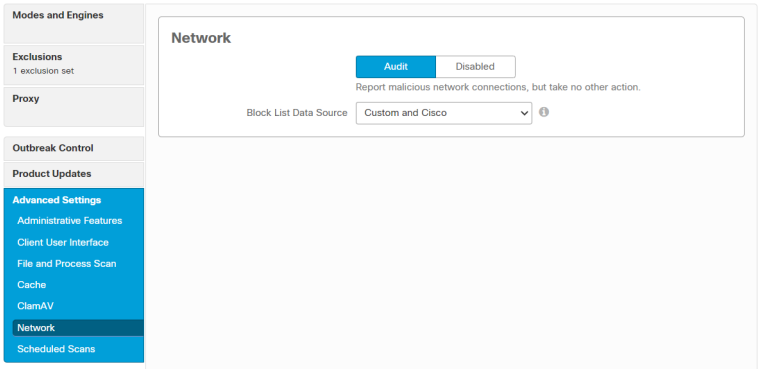
ClamAV

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.

ClamAV definitions contain signatures to detect malware that affects Linux, macOS, and Windows by default. Use the **AV Definitions** setting to select whether you want to download the full set of ClamAV definitions or a smaller subset of definitions that only contains signatures for Linux malware. Select the definitions most appropriate for your environment, including the types of files you expect to be scanned. See Secure Endpoint: ClamAV Virus Definition Options in Linux for more information.

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. You can view the version of ClamAV definitions and update status for a computer from the Computer Management page.

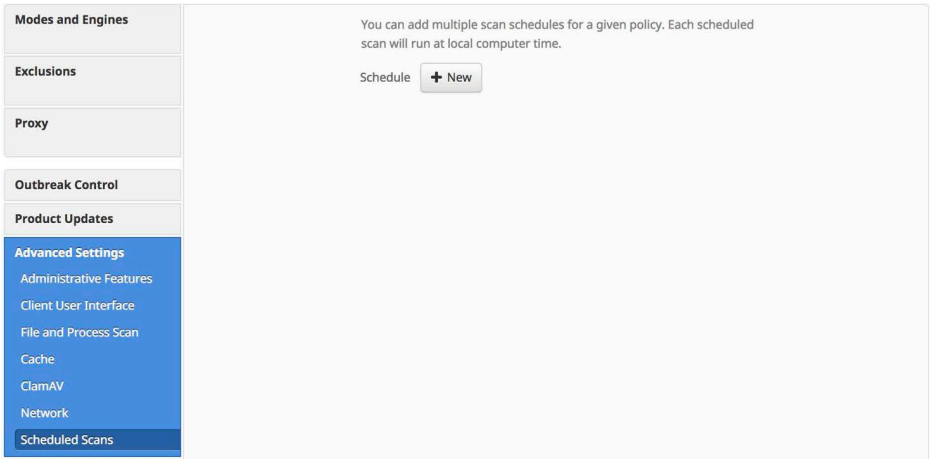
Network



The Network tab contains settings to for the network flow capabilities of your connector, such as device flow correlation settings. You can select to disable Device Flow Correlation or select Audit to log network connections.

Blocked List Data Source enables you to select the IP blocked lists your connectors use. If you select **Custom**, your connectors will only use the IP blocked lists 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 Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos 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 blocked lists you have added to the policy and the Cisco Intelligence Feed.

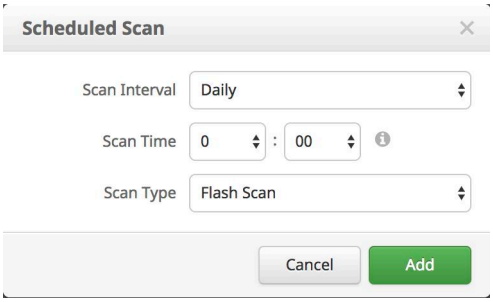
Scheduled Scans



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 7 days 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 **+New under 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. A **Custom** scan will scan a particular path that you give it.

Secure Endpoint Android Connector Policy

This section describes the policy options that are available for Secure Endpoint Android connectors.

Android Connector: Required Policy Settings

Clicking New Policy will take you to the new Secure Endpoint Android policy. The settings on these pages are described below. A policy for the Secure Endpoint Android connector contains fewer options due to the nature of the device.

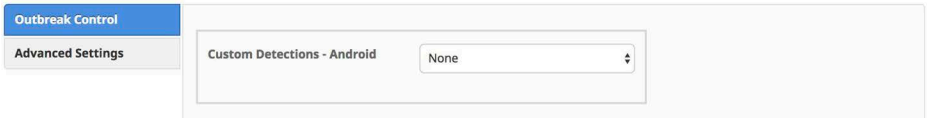
Name and Description

The Name box enables you to create a name that you can use to recognize the policy. You can add more details about the policy in the optional **Description** box.

Android Connector: Other Policy Settings

Once you have filled out the Name and Description you will be able to access pages for Outbreak Control and Advanced Settings. The following sections describe the settings.

Outbreak Control



The Custom Detections - Android list type is described in the Outbreak Control section of this document.

Advanced Settings

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 Secure Endpoint under Applications. For more information on Defense Center integration with Secure Endpoint, see your Defense Center documentation.

Network Policy: Required Policy Settings

Clicking New Policy will take you to the new Secure Endpoint Network policy. The settings on these pages are described below. A policy for the Secure Endpoint Network contains fewer options due to the nature of the device.

Name and Description

The Name box enables you to create a name that you can use to recognize the policy. You can add more details about the policy in the optional **Description** box.

Network Policy: Other Policy Settings

Once you have filled out the Name and Description you will be able to access pages for Outbreak Control. The following section will describe the settings.

Outbreak Control

Custom detections are explained in the Outbreak Control section of this user guide. Allowed lists are explained in the Application Control - Allowed Applications section.

Secure Endpoint iOS Connector Policy

This section describes the policy options that are available for Secure Endpoint iOS connectors with Clarity.

iOS Connector: Required Policy Settings

Clicking New Policy will take you to the new Secure Endpoint iOS policy. The settings on these pages are described below. A policy for the Secure Endpoint iOS connector contains fewer options due to the nature of the device. Many settings for the connector are handled through the Mobile Device Manager (MDM).

Name and Description

The Name box enables you to create a name that you can use to recognize the policy. You can add more details about the policy in the optional **Description** box.

Modes and Engines

This page contains settings pertaining to network conviction modes.

Conviction Modes

Conviction Modes specify how the Clarity module of the Secure Endpoint iOS connector responds to suspicious network activity. There are three modes available:

- **Active Block** checks that the traffic is not destined to a malicious or blocked address before allowing the connection. This provides the highest level of security but there will also be latency with each network connection.

  IMPORTANT! Even in Active Block mode connections will eventually be allowed if the device is unable to reach the Cisco cloud to check the disposition of the destination address.

- **Block** allows network connections while simultaneously checking if the destination address is malicious or blocked. The initial connection will be allowed but all subsequent connections to a malicious or blocked site will be blocked.
- **Audit** will allow all connections but any connections to malicious or blocked sites will be logged.

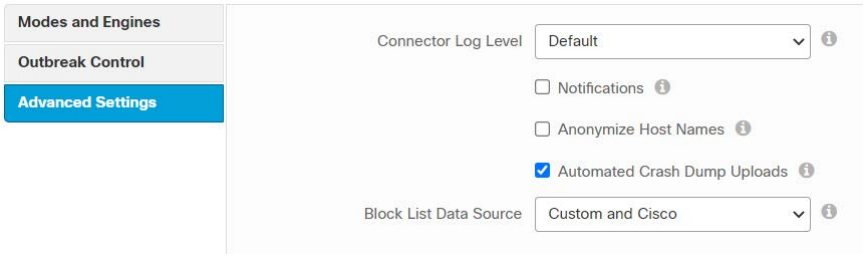
iOS Connector: Other Policy Settings

Once you have filled out the required configuration pages you will be able to access pages for **Outbreak Control** and Advanced Settings. The following section will describe the settings.

Outbreak Control

If there are IP allowed or blocked lists available, you can click Select Lists to choose the ones you want to add to the policy. Fill the checkboxes of all the lists you want to add from the drop-down menu. You can add multiple IP lists to a single policy; however, IP allowed list entries will override IP blocked list entries. See IP Blocked & Allowed Lists for details on creating these lists.

Advanced Settings



Connector Log Level allows you to choose between default and debug (verbose) logging levels. Currently, only Default logging is available.

Notifications displays notifications on the end user's device about malicious connections and other events.

Anonymize Host Names will assign an anonymized name to the device to remove any personally identifiable information that is sent to the Cisco Cloud.

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

Blocked List Data Source enables you to select the IP blocked lists that your connectors use. If you select **Custom**, your connectors will only use the IP blocked lists 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 Talos to have a poor reputation. All the IP addresses in this list are flushed every 24 hours. If Talos 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 blocked lists you have added to the policy and the Cisco Intelligence Feed.

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 Group Menu

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

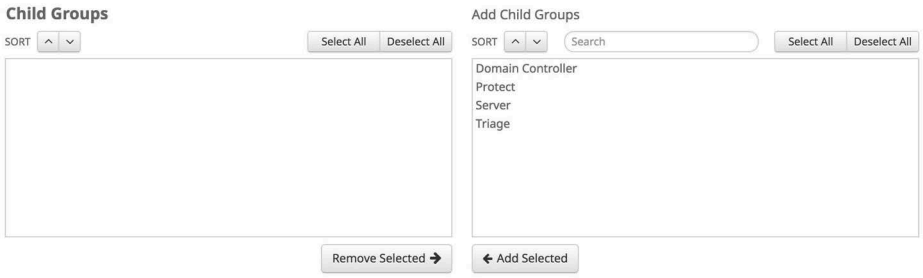
Policy Menus

The policy menus allow you to specify which policies to apply to the group you are creating. Default policies 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 policies 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 select individual groups, multiple groups, or all the groups to add or remove as child groups.



IMPORTANT! If you remove a child group that inherits its policy from its parent, then that group's policy will revert to the organization 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.

IMPORTANT! You cannot move an iOS device to a new group from the Secure Endpoint console. To move a single device you must use the Meraki Dashboard to re-tag the device to the profile with the linked group. You can also re-deploy the device to a new profile. On other MDMs you will have to uninstall the Secure Endpoint iOS connector and install it again for the new Group.

Chapter 7
Deploying Connectors

After you have created policies and assigned them to groups, you can begin deploying the connectors to computers and devices in your organization. Navigate to **Management > Download connector** to deploy the connector to Windows, Mac, Linux, or Android. To deploy the Secure Endpoint iOS connector navigate to **Management > Deploy Clarity for iOS**.

Download Connector

The Download Connector page allows you to download installer packages for each type of connector or copy the URL from which they can be downloaded once you have selected a group. 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.

Secure Endpoint Windows Connector

To deploy the Secure Endpoint Windows connector, first select a group from the drop-down menu. You will be able to see the connector version that will be downloaded as specified in the policy you selected or the default for your organization, and 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. To install the 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 Secure Endpoint Windows 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 Secure Endpoint Windows connector. This executable downloads and installs the appropriate version of the Secure Endpoint Windows 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 Secure Endpoint Windows connector to cisco.com addresses for connectivity, the bootstrapper will not work. You must download the redistributable installer for those operating system versions.

Secure Client

You can download the Cisco Secure Client full installer if you have enabled Cisco XDR or SecureX Integration. Secure Client allows you to deploy the Secure Endpoint Windows connector and Secure Client VPN from a single package. If you select a group that has not already been configured in Cisco XDR or SecureX the Secure Client installer will only contain the Secure Endpoint connector with the default Cloud Management settings. You can go to the Cisco XDR or SecureX console after to configure additional settings and add the AnyConnect VPN module. See https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm or https://securex.us.security.cisco.com/help/insights/topic/secure-client for more information on configuring Secure Client.

Secure Endpoint Mac Connector

To deploy the Secure Endpoint 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 or DMG file to install the Secure Endpoint Mac connector or copy the download link. The installer can be placed on a network share. The file also contains a policy.xml file that is used as a configuration file for the install.

Secure Endpoint Linux Connector

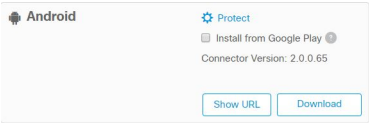
To deploy the Secure Endpoint Linux connector first select a group from the drop down menu. Choose whether to have the connector perform a flash scan during the install process. The flash scan checks processes currently running in memory and should be performed on each install.

Use the **Distribution** pulldown to select the proper connector version for your distribution. See Cisco Secure Endpoint Linux Connector OS Compatibility for supported distributions.

You can then **Download** the rpm or deb file to install the Secure Endpoint Linux connector or copy the download link. The installer can be placed on a network share. The file contains a policy.xml file that is used as a configuration file for the install. You should also copy or download the GPG Public Key linked on the download page. This will be required for Linux Connector: Product Updates via policy.

Secure Endpoint Android Connector

The Secure Endpoint Android connector can be deployed by downloading the app from the Secure Endpoint Console, emailing a link to the app download, or through the Google Play Store.



Select a group on the **Download Connector** page. You can click **Show URL** to copy a link to the APK that can be emailed to users or click Download to download the APK to distribute through a Mobile Device Manager (MDM).

Check **Install from Google Play** if your users will download and install the app themselves. Click **Show Activation URL** to display the activation link that will be emailed to users. This link is also used for the `amp_provisioning_url` value if you deploy using the EMM API to deploy via a Managed Configuration. Users will have to click the activation link from the device with the Secure Endpoint Android connector installed on it to receive a policy and enable the connector. Users who install the app through Google Play will receive connector updates depending on the Play Store app **Auto-update apps** setting.

IMPORTANT! The Secure Endpoint Android connector will not have a policy or protect the device if users install it from Google Play without clicking the activation link from their device.

Managed Configuration

You can also deploy the Secure Endpoint Android connector in a managed configuration through any Mobile Device Manager (MDM) or Enterprise Mobility Manager (EMM).

The managed configuration schema is embedded within the app and can be retrieved using the Google EMM API.

Bootstrapping the connector

To bootstrap the connector the EMM has to specify the activation URL from the **Download Connector** page as a string in `amp_provisioning_url`. The connector will retrieve the specified policy from the Cisco cloud for further cloud connections if this value is present. You can also supply the user with the provisioning URL through other means if you do not specify the value through the EMM API.

Provisioning device name

You can also provision the connector device name by specifying it as a string in `amp_device_name`. The string should be between 3 and 63 characters in length and will be the name that appears for the device in the Secure Endpoint console. This field is optional and if it isn't specified the user will be prompted to enter the device name during registration.

Deploy Clarity for iOS

Deployment steps for the Secure Endpoint iOS connector with Clarity are dependent on the Mobile Device Manager (MDM) you are using. Before you can deploy the Secure Endpoint iOS connector you have to set up your MDM Integration.

Deploy via Meraki

Navigate to **Management > Deploy Clarity for iOS** to make changes to your Meraki deployment. You can apply your Secure Endpoint groups to your Meraki SM profiles. Only one group and its associated policy can be applied to each profile.

1. Select the Secure Endpoint **Group** you want to apply or update on your Meraki SM.
2. Select the **Organization** from your Meraki SM you want to apply it to.
3. Select the **Network** in the Organization.
4. Select one or more **Profiles** that you want to apply Clarity to. For more information on creating profiles see Configuration Profiles.

   IMPORTANT! While you can deploy more than one profile to an iOS device, if you try to deploy more than one profile with Clarity applied an error will occur and the second profile will not be applied. You can safely deploy a second profile with only Clarity applied to a device that has an existing profile that only has Umbrella applied.

5. Click **Update** to deploy.

Once you have deployed the Secure Endpoint iOS connector you will need to use the Meraki Dashboard to deploy the app to devices using the instructions in the document Using Apple's Volume Purchase Program (VPP) with Systems Manager.

If you want to configure notifications,

1. Go to System Manager > Settings.
2. Click Add Profile.
3. Select Device profile (default) and click Continue.

4. Name the profile and enter a description.
5. Select appropriate Target Scope and Device Tags.
6. Click Add settings.
7. Search for “Notification” in the search bar.
8. Click iOS App Notifications.
9. In the App drop-down menu, choose Cisco Security Connector (com.cisco.ciscosecurity.app).

   Fill all the checkboxes and select Banner for Alert type.
10. Click Save.

Deploy via Workspace ONE

To deploy from Workspace ONE you will first need to download a Mobileconfig file from the Secure Endpoint Console:

1. Go to **Management > Deploy Clarity for iOS**.
2. Select the Secure Endpoint **Group** you assigned your iOS policy to previously.
3. Click **Copy to Clipboard**.

IMPORTANT! If you want to exclude domains from being sent to the Cisco Cloud see steps 2 and 3 under Clarity Domain Exclusions for Workspace ONE before continuing.

You will now have to add the Mobileconfig file from your Workspace ONE Dashboard:

1. Navigate to **Devices > Profiles & Resources > Profiles**.
2. Click **Add > Add Profile**.
3. Click iOS.
4. Under General:
   - Assign a **Name** and **Description**.
   - Set **Deployment** to Managed.
   - Set **Assignment Type** to Auto.
   - Set **Allow Removal** to Always.
   - Add the Group you previously created to **Assigned Groups**.
5. Paste the contents of your clipboard into the **Custom Settings** text box.
6. Click Notifications.
7. Click Configure.
8. Click Select App.
9. In the Select App field, choose Cisco Security Connector (com.cisco.ciscosecurity.app).
10. Fill all the checkboxes and select Banner for Alert Style when unlocked.
11. Click Save.
12. Click **Save & Publish**.
13. Under **View Device Assignment** you should see the devices in the Group.

14. Click **Publish**.

IMPORTANT! If you do not want to configure notifications, skip steps 6–11.

Deploy via MobileIron

To deploy from MobileIron you will first need to download a Mobileconfig file from the Secure Endpoint Console:

1. Go to **Management > Deploy Clarity for iOS**.
2. Select the Secure Endpoint **Group** you assigned your iOS policy to previously.
3. Click **Download MobileIron Profile**.

IMPORTANT! If you want to exclude domains from being sent to the Cisco Cloud see steps 2 and 3 under Clarity Domain Exclusions for MobileIron before continuing.

You will now have to add the Mobileconfig file from your MobileIron Dashboard:

1. Navigate to **Policies & Configs > Configurations**.
2. Click **Add New > iOS and OS X > Configuration Profile**.
   - Assign a **Name** and **Description** to the Configuration Profile.
   - Click **Browse** and navigate to the Mobileconfig file you downloaded from the Secure Endpoint Console.
   - Click **Save**.
3. Select the Configuration Profile you just created.
4. Click **Actions > Apply to Label**.
   - Select the Label you created earlier.
   - Click **Apply**.
5. Click **Ok** on the dialog.

If you want to configure notifications,

1. Navigate to **Policies & Configs > Configurations**.
2. Click **Add New > iOS and OS X > Configuration Profile**.
   - Assign a **Name** and **Description** to the Configuration Profile.
   - Click Add+.
   - Choose Cisco Security Connector (com.cisco.ciscosecurity.app) in Bundle Identifier.
   - Fill all the checkboxes and select Banner for Alert Type.
   - Click **Save**.

Deploy via Other MDMs

1. Go to **Management > Deploy Clarity for iOS**.
2. Select the Secure Endpoint **Group** you assigned your iOS policy to previously.

   Click **Download Profile**.

You can now upload the Mobileconfig file to your MDM through the MDM's console to complete deployment.

Deployment Summary

The Deployment Summary page gives you a list of the successful and failed 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 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 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 connector. The top of the page displays a summary of some key computer metrics, such as how many computers require AV and connector updates, and how many computers have faults requiring attention. **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 receive an email with a download link for 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.

Click on a computer in the list to expand details for that computer. Click the **+** or **-** buttons to 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. You can also launch an Orbital Query or take a Forensic Snapshot. Remote Uninstall allows you to uninstall the connector from individual endpoints.

Note that the Last Seen time is accurate within approximately 15 minutes. 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 connector from the computer you will still see events generated by a deleted computer and it will still use one of your available licenses.

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.

Kenna Risk Score

The Kenna Risk Score is represented on a scale from 0-100. It quantifies the risk of a vulnerability by looking at the technical severity and how real-world attackers are leveraging the vulnerability in the wild. A variety of vulnerability and threat variables are considered when calculating this score, including predictive modeling to forecast the weaponization of vulnerabilities, the availability of recorded exploits or exploit kits, the presence of near real-time exploitation, and other variables.

To assess and score vulnerabilities in Secure Endpoint, Kenna Inference maps software running in your environment (i.e. OS vendor, name, version, etc.) to NIST's National Vulnerability Database (NVD) and other knowledge bases to identify related CVEs. A unique Kenna Risk Score is calculated for each of those CVEs using the same data science-based algorithms and vulnerability intelligence that underlie Kenna's flagship vulnerability management platform. CVEs with a Kenna Risk Score of 33 or higher are analyzed for validation.

You can filter the Computers list by Kenna Risk Score and sort the list by ascending or descending score.

Click on the risk score to view the list of CVEs associated with the computer. Each CVE includes:

- The Kenna Risk Score.
- The Common Vulnerability Scoring System (CVSS) 2 score.
- Description of the CVE.
- The properties affected by the vulnerability.

The Fix Available button will show a list of links to fixes for the vulnerability if one exists.

IMPORTANT! Computers running Windows 10 IoT Enterprise are not currently supported.

Save and Manage Filters

It can be useful to save filters to quickly recall for future use. To save a filter, click Apply and Save after selecting the filter parameters. Enter a name for the filter in the following Save Filter dialog and click Save.

You can apply saved filters by selecting from the drop-down list on the Computers page. Save any changes to the current filter by clicking Update.

You can rename the current filter by clicking on the filter's name in the top left of the filters interface. You can also remove the filter by clicking Delete.

Computer Management: Connector Diagnostics

You can remotely trigger diagnostics of a computer by clicking the Diagnose... button in the expanded computer details view in the Inbox Tab, Device Trajectory, or the Computer Management page. You can use this if you believe your connector is not functioning correctly and either attach the diagnostic file to a support ticket or perform your own analysis.

Computers require the following minimum versions of the connector to remotely collect diagnostics with this feature:

- Windows: 6.2.1
- Mac: 1.9.0
- Linux: 1.9.0
- iOS: 1.2.0

IMPORTANT! Diagnostics can still be gathered locally from earlier versions of the connector.

This generates a diagnostic file containing debug logs that you can download and view from the File Repository.

IMPORTANT! Because this feature requires access to the File Repository, the user triggering connector diagnostics must have Two-Factor Authentication enabled on their account and have privileges to fetch files from the File Repository. (See Users can access their account settings on this page by clicking My Account.)

You can select the length of the debug session from the drop-down menu and choose options for the diagnostics.

IMPORTANT! The options available vary depending on the operating system of the device.

Filling the Historical Data checkbox for Windows computers collects log files that existed prior to the request. On Linux and Mac computers, enabling this option prevents log rotation for the duration of the debug session.

Filling the Kernel Log checkbox for Windows computers collects extra log files generated from kernel drivers. On Linux and Mac computers, enabling this option enables verbose logging for kernel modules.

Filling the Include cache database checkbox for iOS devices collects data from web service requests.

Filling the Include Umbrella Logs checkbox for iOS devices collects all Umbrella component logs.

Once you have selected the desired options, click Create. If you have chosen to receive announcements by email (see Users), you will receive an email when the diagnostic file is ready to download from the File Repository.

IMPORTANT! It can take up to 24 hours for the diagnostic file to generate.

To access diagnostic files, you can click Diagnostics, which takes you directly to the File Repository page filtered by connector diagnostics.

Computer Management: Secure Endpoint iOS Connector

Click the name of an iOS device to view its details.

From the details you can click to view all **Events** associated with the connector, the **Device Trajectory**, and the **Audit Log** for that device. You can also delete the device. The Move button is disabled because you cannot move an iOS device using the Secure Endpoint Console. To move a single device you must use the Meraki Dashboard to re-tag the device to the profile with the linked group. You can also re-deploy the device to a new profile.

View Changes will take you to a filtered view of the Audit Log, which shows all changes for the specific computer. You can also click the **Events** link to open a filtered Events Tab view for the selected computer.

IMPORTANT! You cannot move an iOS device to a new group from the Secure Endpoint Console. To move a single device you must use the Meraki Dashboard to re-tag the device to the profile with the linked group. You can also re-deploy the device to a new profile. On other MDMs you will have to uninstall the Secure Endpoint iOS and install it again for the new Group.

Chapter 8
Secure Endpoint Windows Connector

After you have defined groups, policies, and a deployment strategy, the Secure Endpoint Windows 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. See Connector Engines and Features for the connector capabilities.

Windows System Requirements

The following are the minimum system requirements for the Secure Endpoint Windows connector for desktop computers and servers. The Secure Endpoint Windows connector supports 64-bit versions of these operating systems on x86 processors. Additional disk space may be required when enabling certain connector features. These are the Secure Endpoint Windows connector requirements, and do not take into account Windows system requirements.

- 2 GB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space – TETRA
- For CPU recommendations, please refer to the Microsoft recommended requirements

See Secure Endpoint Windows Connector OS Compatibility for operating system compatibility.

Incompatible Windows Software and Configurations

The Secure Endpoint Windows connector is currently not compatible with the following software:

- ZoneAlarm by Check Point
- Carbon Black (only incompatible with connector versions 6.3.5 and earlier)
- Res Software AppGuard

The Secure Endpoint Windows connector does not currently support the following proxy configurations:

- Websense NTLM credential caching. The currently supported workaround for Secure Endpoint is either to disable NTLM credential caching in Websense or allow the 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 connector.
- Kerberos / GSSAPI authentication. The currently supported workaround is to use either Basic or NTLM authentication.

The malicious activity protection engine is not compatible with Hyper-V clusters.

The Secure Endpoint Windows connector does not support the following configurations on Windows 10 IoT Enterprise:

- HORM and UWF are not supported.
- Kenna Risk Score is not available.

Rootkit scans launched from the connector UI are not compatible with desktop or file virtulization software.

Windows Connector Firewall Exceptions

Firewall exceptions for proper operation of the Secure Endpoint Windows connector can be found in Connector Firewall Exceptions.

Windows 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 connector can be set to discover endpoint proxy settings automatically. Once the connector detects proxy setting information, it attempts to connect to the Secure Endpoint 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 Secure Endpoint 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.

Windows Installer

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

IMPORTANT! If you are running other security products in your environment, there is a possibility that they will detect the Secure Endpoint connector installer as a threat. In order to successfully install the connector, add it to an allowed list/exclude it in the other security products and try again.

Windows Interactive Installer

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

If Windows User Access Control (UAC) is enabled, the user is presented with a prompt and should select **Yes** to continue.

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

1. The install location dialog appears. 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.
2. When the install is complete, click Next to continue.
3. 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 executes. The Windows System Tray icon indicates you are now connected to the Cisco Cloud if you selected Cloud Notifications in the policy applied to the connector.
4. When the scan has completed, click Close to complete all install steps. The connector is now running on the endpoint.

Windows 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 device flow correlation driver.

IMPORTANT! Any connectors installed using this flag must be in a group with a policy that has **Modes and Engines > Network** set to **Disabled**.

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

IMPORTANT! Any connectors installed using this flag must be in a group with a policy that has **Modes and Engines > TETRA** unchecked.

- /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.

IMPORTANT! Do not use the /overridepolicy switch to move computers from one group to another. Instead, use the Secure Endpoint Console. For details, see Adding and Moving Computers.
When you have computers in different groups and all computers need to be upgraded to a new connector version without overriding their policy settings, use /overridepolicy with the non-default value: "/overridepolicy 0".

- /temppath – Used to specify the path to use for temporary files created during connector install. For example, /temppath C:\somepath\temporaryfolder. This switch is only available in the Secure Endpoint Windows connector 5.0 and higher.

  IMPORTANT! The following switch for skipping registration and startup of connector is intended for use when creating a Windows operating image as a deployable golden image.

- /goldenimage 1 – Skip initial connector registration and startup on install.
- /goldenimage 0 – Do not skip initial connector registration and startup on install.

IMPORTANT! Starting with Secure Endpoint Windows connector version 6.3.1, if using any installer switch that contains a path argument (e.g. /temppath, /D switches) that contains a single quote character ('), you will need to enclose the entire path in double quotes ("). If not, the installer will incorrectly parse the argument and install the connector in a different location than expected.

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 Secure Endpoint 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.

Secure Endpoint Windows connector 6.0.5 and higher has a command line switch to skip the check for Microsoft Security Advisory 3033929.

- /skipexprevprereqcheck 1 – Skip the check for Microsoft Windows KB3033929.
- /skipexprevprereqcheck 0 – Check for Microsoft Windows KB3033929 (Default).

IMPORTANT! If you use this switch and do not have this KB installed, or other Windows Updates that enable SHA-2 code signing support for Windows 7 and Windows Server 2008 R2, you will encounter issues connecting to the Cisco Cloud.

Secure Endpoint Windows connector 6.0.7 and higher has a command line switch to set the registry key necessary to receive the Windows Security Update for KB 4072699.

- /kb4072699 1 – Set the registry key value.
- /kb4072699 0 – Do not set the registry key value (Default).

IMPORTANT! The registry key value can only be set using this command line switch. If you do not set this key either using the switch or manually, you will not receive the patch. See Cisco Secure Endpoint Compatibility with Windows Security Update KB4056892 for a list of compatible versions.

Secure Endpoint Windows connector 7.0.5 and higher should no longer require a reboot to complete any upgrade to a later version. However, there may be instances where this can happen unexpectedly, so the installer has a choice to either move forward and complete the upgrade (but will require a reboot), or fail the upgrade and roll back everything to its previous state/version.

- /overrideupgradefailure 0 – If the upgrade encounters an issue where it isn't able to continue without rebooting, the upgrade will rollback all changes and send an upgrade failed event.
- /overrideupgradefailure 1 – If the upgrade encounters an issue where it isn't able to continue without rebooting, the upgrade will continue and a reboot will be required to complete the upgrade.

Windows Installer Exit Codes

Installer exit codes and descriptions can be found in this TechNote.

Cisco Security Monitoring Service

With versions of Secure Endpoint Windows connector lower than 6.3.1, the connector registers itself with Windows Security Center (WSC) when the TETRA engine is enabled and its definitions are up to date. Once it is successfully registered, Windows Defender will be disabled and Secure Endpoint will be designated as the active Virus and Threat Protection provider.

Starting with Secure Endpoint Windows connector 6.3.1, the Cisco security monitoring service will now be responsible for registering with WSC. As an anti-malware protected process light (AM-PPL) service, it will be able to communicate with WSC to enable or disable Windows Defender according to TETRA's status.

IMPORTANT! Windows Defender cannot be automatically disabled in Windows Server versions 2016 and later. If you want to run TETRA on those operating systems you must disable Windows Defender manually.

Windows Connector User Interface

When the connector is installed you can access it by double-clicking the desktop shortcut, clicking the Cisco Secure Client entry in the Windows Start menu, or launching it from the Windows tray.

The user interface supports up to eight concurrent users on the endpoint (connector version 8.1.3 and later). If a ninth concurrent user attempts to open the client user interface, it will launch but appear to be disabled. The connector will still be running and providing protection for all users.

From the connector main screen you can choose to launch a scan and 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

Select a scan type from the pulldown and click Start to initiate a scan.

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.

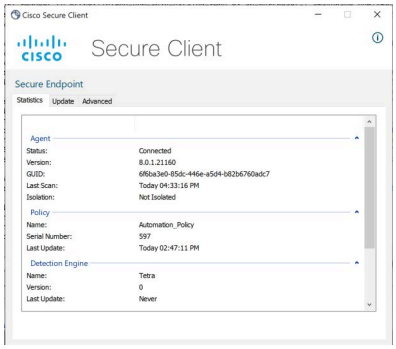
Full Scan: Scans the entire computer including all attached storage devices (such as USB drives). This scan can be time-consuming and resource-intensive, so should only be performed once when the connector is first installed.

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.

IMPORTANT! Rootkit scans are not compatible with desktop or file virtulization software.

Settings

Click the cog icon to view the settings screen that is divided into Statistics, Update, and Advanced tabs. The Diagnostics button should only be used at the request of support as part of troubleshooting connector issues.



The Statistics tab provides information about the connector, including the policy name and serial number, TETRA engine information, and proxy settings. This can be useful for troubleshooting and support sessions.

The Update tab lets you initiate a check for and install updates to policy, software, and detection engine signatures.

The Advanced tab lets you start Debug Logging and view the Event History. Debug logging should only be used at the request of support as part of troubleshooting connector issues as it can consume system resources. The Event History button will launch the Windows Event Viewer to show informational and error events generated by the connector. This includes detection and quarantine events.

IMPORTANT! Information for the AnyConnect VPN module will also be displayed in Settings when Secure Client is installed.

Windows Connector Command Line Interface

You can also use and manage aspects of the connector from the command line interface. The executable is located at `<install path>\<version>\sfc.exe` where the install path is the path you specified during install and version is the version number of the connector. For example, the default path for version 8.0.1 of the connector would be:

```
%Program Files%\Cisco\AMP\8.0.1.21160\sfc.exe
```

IMPORTANT! You must specify the full path when using the command line interface.

Useful commands include:

- `sfc.exe -s` - start the connector service.
- `sfc.exe -k <password>` - stop the connector service where <password> is the Connector Protection password.

- `sfc.exe -l start` - start local debug logging. Debug logging does not persist across restarts of the service or reboots of the computer.
- `sfc.exe -l stop` - stop local debug logging.
- `sfc.exe -forceUpdate` - check for product and definition updates.

IMPORTANT! You must have administrator privileges to run the connector CLI commands.

Windows Connector Support Tools

The Secure Endpoint Windows connector includes tools to assist in troubleshooting connector issues.

Windows 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].zip 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.

Windows 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].zip 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.

Windows 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 Secure Endpoint 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. You must include a space between the switch and the 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.
/HC	Perform a connectivity test with the registration server.
/UH	Perform a connectivity test with the update server. Only run when an update is configured via policy.
/R	Perform a connectivity test with the remote file fetch server.
/O	Perform a connectivity test with Orbital servers. Only available when Orbital is enabled in the organization.
/BPD	Performs Behavioral Protection server and XML connection tests.
/BPU	Performs Behavioral Protection upload test.

If you run the tool without specifying any switches it runs with all switches enabled.

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

Uninstall the Windows Connector

You must uninstall the connector to reclaim the license so it is available for another endpoint. To uninstall a connector from an endpoint:

1. Navigate to the Control Panel.
2. Under Programs select Uninstall a program.
3. Select **Cisco Secure Endpoint** in the program list, then click Uninstall/Change.
4. Click the Uninstall button on the dialog box to remove the application.
5. If a password requirement to uninstall the connector has been set in Policy you will be prompted to enter it.
6. 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 connector history and quarantine files. Reboot the computer to complete the uninstall

process if prompted. If you are uninstalling connector versions 7.0.5 and later the computer should not require a reboot under most conditions.

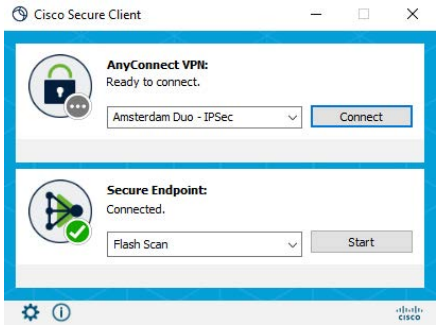
IMPORTANT! On Windows 8 and higher, if Fast Startup mode is enabled and you are prompted to reboot, you should reboot the computer after uninstall is complete rather than using the Windows shutdown option. This will ensure that the final cleanup steps to remove the connector drivers complete properly.

Cisco Secure Client

Cisco Secure Client allows you to deploy the Secure Endpoint Windows connector and Secure Client VPN to endpoints as a single package managed by a cloud management module.

You will have to enable Cisco XDR or SecureX Integration to use Secure Client. Once the integration has been activated, you will be able to download the full Secure Client installer from the Download Connector page in the Secure Endpoint console or from the Cisco XDR or SecureX console. See https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm or https://securex.us.security.cisco.com/help/insights/topic/secure-client for more information on configuring additional Secure Client settings and adding the AnyConnect VPN module.

IMPORTANT! When you enable Secure Client in Cisco XDR or SecureX, read/write API Credentials are created in your Secure Endpoint organization so an install token can be created.



The Secure Client user interface is the same as the Windows Connector User Interface with the addition of AnyConnect VPN module settings.

The Secure Endpoint part of the user interface supports up to eight concurrent users on the endpoint (connector version 8.1.3 and later). If a ninth concurrent user attempts to open the client user interface, it will launch but appear to be disabled. The connector will still be running and providing protection for all users. The other Secure Client module user interfaces do not currently support concurrent users.

Secure Client 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:

- -c or --cleanup - Enable removal of the temp directory on exit. Use -c=false to preserve the temp directory even if install succeeds. The default is -c=true.
- -d or --debug - Enable debug output.
- -la - List install actions to be run.
- -ls - List embedded files.
- -lsjson - List embedded files (JSON output).
- -q or --quiet - Run the installer silently. This option will also need to be used to install Secure Client on any computers with invalid or outdated display drivers.
- -v or --verbose - Enable verbose output.

Chapter 9
Secure Endpoint Mac Connector

After you have defined groups, policies, and a deployment strategy, the 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. See Connector Engines and Features for the connector capabilities.

MacOS System Requirements

The following are the minimum system requirements for the Secure Endpoint Mac connector. These are the Secure Endpoint Mac connector requirements, and do not take into account the Mac system requirements.

- 1 GB RAM
- 1 GB available hard disk space

See Verify Secure Endpoint Mac Connector OS Compatibility for operating system compatibility.

Incompatible macOS Software and Configurations

The Secure Endpoint Mac connector does not currently support the following proxy configurations:

- Websense NTLM credential caching: The currently supported workaround for Secure Endpoint is either to disable NTLM credential caching in Websense or allow the 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 connector.
- Kerberos / GSSAPI authentication: The currently supported workaround is to use either Basic or NTLM authentication.

Mac Connector Firewall Exceptions

Firewall exceptions for proper operation of the Secure Endpoint Mac connector can be found in Connector Firewall Exceptions.

Mac Connector Proxy Autodetection

The connector is able to use multiple mechanisms to support anonymous proxy servers. A specific proxy server can be defined in Policies or the connector can discover endpoint proxy settings defined in a proxy auto config (PAC) file. The location (URL) of this file is set in macOS network adapter settings.

When the proxy type is set in policy to Automatic Proxy Configuration, and Automatic Proxy Configuration is enabled on the endpoint with a URL to a valid pac file, the connector can discover these endpoint proxy settings automatically. Once the connector detects proxy setting information, it attempts to connect to the Secure Endpoint Management Server to confirm that the proxy server settings are correct. The connector will attempt to retrieve the settings only from system-wide settings and not per-user settings.

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/xjavascript-config must be specified. Since all connector communications are already encrypted, https proxy is not supported.

The connector will attempt to rediscover proxy settings every 30 minutes or 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.

See Secure Endpoint Mac Proxy Automatic Configuration (PAC) Setup Guide for more information.

Installing the Secure Endpoint Mac Connector

The Secure Endpoint Mac connector is distributed in two formats:

- macOS install package (.pkg)
- Apple disk image (.dmg)
- To install the Mac connector that is distributed as a .pkg file, double-click the file to start the installation process.
- To install the Mac connector that is distributed as a .dmg file, double-click the file to open the disk image and follow the on-screen instructions.

Alternatively, you can also install the pkg file from the terminal using the installer command. For more information, type `man installer` from the terminal.

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 40 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. Click Finish to complete the Secure Endpoint Mac connector installation.

IMPORTANT! Starting with connector version 1.10.0, file scan operations are performed using an unprivileged process. During connector installation, a user and group named `cisco-amp-scan-svc` are created on the system. If this user or group already exists but is configured differently, then the installer will attempt to delete and then re-create them with the necessary configuration. The installer will fail if the user and group could not be created with the necessary configuration.

TIP! Review `/var/log/install.log` for details on connector installation failures.

IMPORTANT! If you are running other security products in your environment, there is a possibility that they will detect the Secure Endpoint connector installer as a threat. In order to successfully install the connector, add it to an allowed list/exclude it in the other security products and try again.

Install the Secure Endpoint Mac Connector through Automation

To install the connector using a script or other automation, use a workflow similar to the following steps:

1. Download amp_<groupname>.dmg from the Secure Endpoint Console.
2. Push amp_<groupname>.dmg to your endpoints.
3. Mount the .dmg file.

   ```
   $ hdiutil attach amp_<groupname>.dmg
   ```
4. Execute the Apple notarized Mac connector package file.

   ```
   $ sudo installer -pkg /Volumes/ampmac_connector/
   amp_<groupname>.pkg -target /
   ```
5. Un-mount the .dmg file

   ```
   $ hdiutil detach /Volumes/amp_<groupname>
   ```

Grant User Approval after Installing the Secure Endpoint Mac Connector

The Mac connector requires the following user approvals to operate correctly:

- System Extensions (macOS 10.13 and later)
- Full Disk Access (macOS 10.14 and later)

Approve the System Extension

macOS 10.13 introduced a change that requires user consent before an application can run a system extension. The connector uses a system extension to monitor file system and network activity. When the connector starts but approval has not been granted, a message will be displayed indicating a system extension signed by Cisco is blocked. Follow the on-screen instructions to open Security and Privacy System Preferences to approve the extension. Two new system extensions were added in Secure Endpoint Mac connector 1.14.0 that need approval on macOS 10.15 and later.

Approve the System Extension with MDM

System extensions can be automatically approved using the Kernel Extension Policy Payload in a Mobile Device Management (MDM) profile for deployment and management. This removes the need for action by the end-user. For Secure Endpoint Mac connector 1.14.0 and later see Advisory for Secure Endpoint Mac Connector on macOS 11 (Big Sur), macOS 10.15 (Catalina, and macOS10.14 (Mojave).

IMPORTANT! The user will have to accept the MDM profile on Macs running macOS 10.13.4 and later if they are not in the Device Enrollment Program (DEP).

Grant Full Disk Access

MacOS 10.14 introduced a change that requires user consent before an application can access user files such as contacts, calendars, photos, mail and messages. Full Disk Access must be granted for the connector to access and scan those files on macOS 10.14 and later.

For Secure Endpoint Mac connector 1.16.0 to 1.16.2

1. Launch System Preferences.
2. Click Security and Privacy.
3. Click the lock to make changes.
4. On macOS 10.14 select Full Disk Access from the left pane and add “AMP for Endpoints Service” by doing one of the following:
   - Click the + button and choose “/Applications/Cisco AMP for Endpoints/AMP for Endpoints Service” in the file selector dialog.
   - Drag “/Applications/Cisco AMP for Endpoints/AMP for Endpoints Service.app” from Finder to the right pane.

   On macOS 10.15 and later select Full Disk Access from the left pane. Different programs will be listed for Mac Connector Full Disk Access depending on the version of the Mac connector being run. Ensure the following are checked if they appear in the list:
   - ampdaemon
   - AMP for Endpoints Service
   - AMP Security Extension

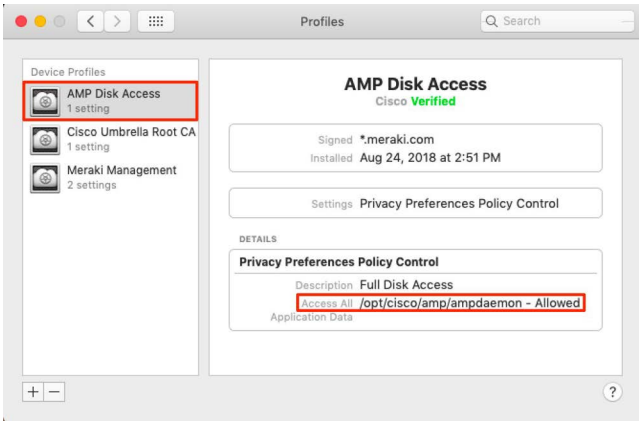
For Secure Endpoint Mac connector 1.18.0 and later

1. Launch System Preferences.
2. Click Security and Privacy.
3. Click the lock to make changes.
4. Select Full Disk Access from the left pane. Different programs will be listed for Mac Connector Full Disk Access depending on the version of the Mac connector being run. Ensure the following are checked if they appear in the list:
   - ampdaemon
   - Secure Endpoint Service
   - Secure Endpoint File Monitor

Grant Full Disk Access with MDM

For customers using a Mobile Device Management (MDM) solution (e.g. Cisco Meraki) for deployment and management, Full Disk Access can be granted using the Privacy Preferences Policy Control Payload in an MDM profile. This removes the need for action by the end-user. For Secure Endpoint Mac connector 1.14.0 and later see Advisory for Secure Endpoint Mac Connector on macOS 11 (Big Sur), macOS 10.15 (Catalina, and macOS10.14 (Mojave).

IMPORTANT! The user will have to accept the MDM profile on Macs running macOS 10.13.4 and later if they are not in the Device Enrollment Program (DEP).



The Cisco Secure Endpoint details are as follows:

- Name: Cisco Systems, Inc. (TDNYQP7VRK)
- Team Identifier: TDNYQP7VRK

Beginning with Secure Endpoint Mac connector 1.9.0, endpoints that have not granted access to the protected paths will send an event that is visible in the Secure Endpoint Console. You can determine which connectors may be operating in a degraded state by reviewing the devices generating this event type.

Using the Secure Endpoint Mac Connector

You can determine the Mac connector's status from the icon's appearance on your Mac's menu bar.

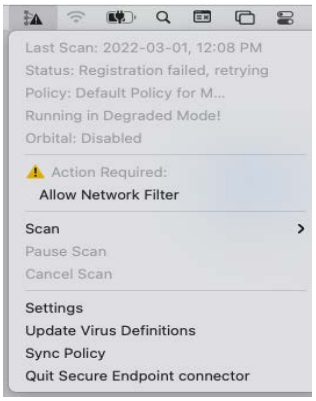
Operational: The connector is connected to the Cisco cloud and the system is protected.

Alert: The connector has encountered an error and is not operating correctly. Protection is off and action is required.

Offline: The connector is disconnected from the Cisco cloud. Protection is limited to the offline engine.

Scanning: A scan is in progress.

Clicking on the icon displays the menulet, which 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.

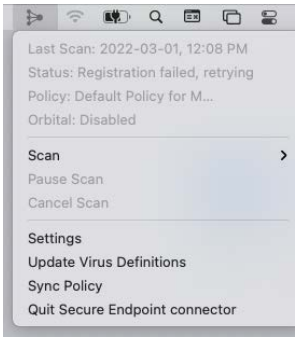


The menulet may also notify you of action that needs to be taken and connector faults.

IMPORTANT! The Secure Endpoint Mac connector uses 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`. 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.

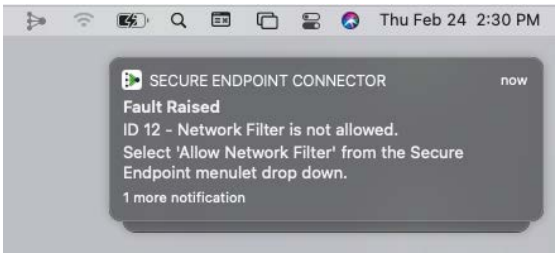
Action Required

The connector icon in the menu bar will flash when the connector requires action to be taken to return to a operational state. When you click on a required action in the menulet, you will be guided on-screen through the process of performing the action.



Mac Connector Faults

The connector may notify you of a Fault Raised event when it detects a condition that affects the proper functioning of the connector. Similarly, a Fault Cleared event communicates that the condition is no longer present. See this Secure Endpoint TechNote for details.



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.

Sync Policy

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.

Mail.app

Email messages containing malware will not be quarantined by the Secure Endpoint 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.

Mac Connector Disabled Status

If the connector status is **Disabled**, contact Support.

Uninstall the Mac Connector

To uninstall the Secure Endpoint Mac connector, navigate to the installation folder Applications > Cisco Secure Endpoint and double-click the **Uninstall Secure Endpoint Connector.pkg** file. Follow the steps in the wizard to uninstall the application. Orbital will be automatically removed as part of the uninstall process if it was enabled.

Because the uninstaller does not remove the `cisco-amp-scan-svc` user and group, run the following two commands to delete the user and group:

```
sudo dscl .-delete /Users/cisco-amp-scan-svc
sudo dscl . -delete /Groups/cisco-amp-scan-svc
```

The Secure Endpoint Mac connector will have to be manually removed if for any reason the uninstaller is not successful. For manual uninstallation, see this TechZone article.

Chapter 10
Secure Endpoint Linux Connector

After you have defined groups, policies, and a deployment strategy, the 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.

Linux System Requirements

The following are the system requirements for the Secure Endpoint Linux connector. The Secure Endpoint Linux connector only supports x64 architectures. These are the Secure Endpoint Linux connector requirements, and do not take into account Linux system requirements or other applications and services.

Using Linux-only ClamAV Definitions

	Minimum	Recommended
Cores	2	4 or more
Memory	1 GB	2 GB
Free disk space in /opt	1 GB	1 GB

Using Full ClamAV Definitions

	Minimum	Recommended
Cores	2	4 or more
Memory	3 GB	4 GB
Free disk space in /opt	2 GB	2 GB

IMPORTANT! The connector installs and maintains temporary files in /opt/cisco/amp/.

See Verify Secure Endpoint Linux Connector OS Compatibility for operating system compatibility. See Cisco Secure Endpoint Linux Connector on Debian-based systems for Debian-based system requirements.

IMPORTANT! The Secure Endpoint Linux connector may not install or run properly on custom and unsupported kernels. If you have a custom kernel, contact Support before attempting to install. If you have an unsupported kernel, you may be able to build kernel modules for that version. See Building Cisco Secure Endpoint Linux Connector Kernel Modules for more information.

Incompatible Linux Software and Configurations

The Secure Endpoint Linux connector is currently not compatible with the following software:

- F-Secure Linux Security on RHEL/CentOS 6.x (See Linux Connector Firewall Exceptions for compatibility on CentOS 7.4)
- Kaspersky Endpoint Security
- McAfee VSE for Linux
- McAfee Endpoint Security for Linux
- Sophos Server Security 9 on RHEL/CentOS 6.x (See Linux Connector Firewall Exceptions for compatibility on CentOS 7.4)
- Symantec Endpoint Protection
- Trend Micro Deep Security Agent

The Secure Endpoint 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 Secure Endpoint Linux connector does not support UEFI Secure Boot on the following operating system versions:

- CentOS 6
- Red Hat Enterprise Linux 6
- CentOS 7
- Red Hat Enterprise Linux 7
- openSUSE Leap 15.1
- SUSE Linux Enterprise 15 SP 1
- Amazon Linux 2
- Oracle Linux 6
- Oracle Linux 7 RHCK

The Secure Endpoint 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 Secure Endpoint from influencing kernel taint, the Secure Endpoint 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 Secure Endpoint service effectively disables Secure Endpoint protection on this system. To disable the Secure Endpoint 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 Secure Endpoint service, run the commands:

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

Linux Connector Firewall Exceptions

Firewall exceptions for proper operation of the Secure Endpoint Linux connector can be found in Connector Firewall Exceptions.

Installing the Secure Endpoint Linux Connector

Execute the following command to install the connector on Debian-based systems:

```
sudo apt-get install [deb package] -y
```

where `[deb package]` is the path to the file on the computer, for example `~/Desktop/amp_Audit.deb`.

Execute the following command to install the connector on other supported distributions:

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

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

Execute the following command to install the connector on SUSE:

```
sudo zypper install -y [rpm package]
```

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

IMPORTANT! There is a possibility that other security products in your environment will detect the Secure Endpoint connector installer as a threat. Add it to an allowed list/exclude it in the other security products and try again if this occurs.

IMPORTANT! File scan operations are performed using an unprivileged process starting with connector version 1.10.0. A user and group named `cisco-amp-scan-svc` are created on the system during installation. The installer will attempt to delete and then re-create this user or group with the necessary configuration if they already exist but are configured differently. The installer will fail if the user and group could not be created with the necessary configuration.

Linux Connector Updates

For connectors in a private cloud environment and connector versions prior to 1.17.0 in a public cloud environment, the Cisco GPG Public Key must be manually imported on the machine after the connector is installed to support updates via policy. You can also copy the GPG Public Key from the Download Connector page to verify the signing of the RPM or DEB. 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 on rpm-based Linux or your debsig keychain on Debian-based systems.

To import the GPG key on rpm-based Linux:

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.

To import the GPG key on Debian-based Linux, follow the steps outlined under the "Verifying the DEB Package" section of the Cisco Secure Endpoint Linux Connector on Debian-based systems article.

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 Secure Endpoint Linux Connector

The Secure Endpoint Linux connector uses a command line interface rather than a graphical user interface on endpoints. The Secure Endpoint 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`.

Linux Connector Faults

The connector may notify you of a Fault Raised event when it detects a condition that affects the proper functioning of the connector. Similarly, a Fault Cleared event communicates that the condition is no longer present. See this Secure Endpoint TechNote for details.

Linux Connector 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`.

Linux Connector Disabled Status

If the connector status is **Disabled**, contact Support.

Uninstall the Linux Connector

Execute the following command to uninstall the Secure Endpoint Linux connector on Debian-based systems:

```
sudo apt-get remove ciscoampconnector -y
```

Execute the following command to uninstall the Secure Endpoint Linux connector on SUSE:

```
sudo zypper remove -y ciscoampconnector
```

Execute the following command to uninstall the connector on other supported distributions:

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

IMPORTANT! yum will remove Orbital as a child dependency if required.

Note that this will leave behind local data including history, quarantined files, and the `cisco-amp-scan-svc` user and group. Run the following script if you do not plan on reinstalling the connector and want to remove the remaining files:

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

IMPORTANT! This will check for Orbital as it is a child dependency and remove it if needed.

If you prefer to use dpkg, specify Orbital to make sure Orbital is removed when needed:

```
sudo dpkg --remove cisco-orbital ciscoampconnector
```

Run the following script if you do not plan on reinstalling the connector and want to remove Orbital:

```
sudo apt-get purge ciscoampconnector -y
```

IMPORTANT! This will check for Orbital as it is a child dependency and purge if needed.

If you prefer to use dpkg, also specify Orbital to make sure Orbital is purged when needed:

```
sudo dpkg --purge cisco-orbital ciscoampconnector
```

IMPORTANT! You can use the Ubuntu Software Center to uninstall the connector but it will not remove local data and configuration. You will still need to run the script above to remove those files.

Chapter 11
Secure Endpoint iOS Connector

The Secure Endpoint iOS connector provides unprecedented visibility by monitoring app use and network activity on supervised iOS devices with a module named Clarity. Clarity is managed within the Secure Endpoint console and is a single location for investigating incidents and device activity across your entire Secure Endpoint iOS deployment. Before you can deploy the Secure Endpoint iOS connector you have to set up your MDM Integration.

For information on installing and configuring Umbrella see the Secure Endpoint iOS Umbrella Setup Guide.

iOS System Requirements

The following are the minimum system requirements for the Secure Endpoint iOS connector:

- The device must be running in supervised mode and managed using a Mobile Device Manager (MDM). See your MDM documentation for further requirements around device settings and configuration.
- 5 MB free space.

You will also have to set up MDM Integration between the Secure Endpoint Console and one of the following Mobile Device Managers:

- Meraki System Manager (SM)
- MobileIron
- IBM MaaS360
- Jamf Pro
- MobiConnect
- Workspace ONE
- Microsoft Intune

See this article for iOS version compatibility.

iOS Connector Known Issues

- Deleting a device in the Secure Endpoint console will not de-provision it in your MDM (either remove the app configuration or the app itself). The workaround is to remove the Secure Endpoint iOS app from devices via the MDM and they will continue to appear in the Secure Endpoint console until manually deleted.
- If installing the Secure Endpoint iOS connector using Apple Configurator, there is a known issue where the serial number is not being populated correctly.
- Devices with some emoji names may not register. Most emoji are handled.
- The Secure Endpoint console is not notified when the app is uninstalled from a device. This means that when the Secure Endpoint iOS connector is uninstalled and reinstalled there will be duplicate entries for that device in the console.
- Identity sync (if enabled) may cause duplicate Secure Endpoint iOS connectors to appear in the console if a device is wiped and the connector is installed again.
- Clarity does not have visibility for per-app VPN or App tunneling traffic, therefore the Secure Endpoint console is not able to display the traffic on Device Trajectory.
- When deploying two profiles to the same device, if both profiles contain the same module (Clarity or Umbrella), then an error is thrown in your MDM and the second profile is not deployed. For example, if profile1 containing only Clarity is deployed first, profile2 containing Clarity and Umbrella won't be deployed, and the app has only Clarity configured in profile1 running. If two profiles do not have any common module, both profiles are deployed. For example, profile1 containing only Clarity is deployed first, then profile2 containing only Umbrella will be deployed as well, and the app has both Clarity and Umbrella running.
- Cisco Security connector 1.2.0 and lower does not have visibility for TOR traffic in Active Block mode and is unable to block the traffic.
- Cisco Security connector version 1.3.0 and higher has visibility into TOR traffic in all modes and is able to block the traffic, but its ability to do so is limited to browsers that disclose IP information.

iOS Connector Firewall Connectivity

The Secure Endpoint iOS connector needs access to certain servers over specific ports if your devices are used on wifi networks behind a firewall. Firewall exceptions for proper operation of the Secure Endpoint iOS connector can be found in Connector Firewall Exceptions.

Clarity Domain Exclusions

A domain exclusion list allows you to specify domains that Clarity will ignore. Any network activity to domains on this list will not be reported to the Cisco cloud and will not appear in Mobile App Trajectory or Device Trajectory. The exclusion list is specified through your Mobile Device Manager dashboard.

Clarity supports exclusions via exact hostname matching or sub-domains using wild cards. For example, you can exclude the exact hostname www.cisco.com or you can exclude the sub-domain *.cisco.com, which will exclude www.cisco.com, cisco.com, and any other sub-domains in the cisco.com primary domain.

Meraki Domain Exclusions

1. On your Meraki dashboard open a profile with the Secure Endpoint iOS connector and select Clarity Content Filter.
2. Add a key domain_exclusions_list and select List from the Type drop down. Add hostnames or sub-domains in the Value field and save your changes. You can add multiple hostnames and sub-domains to the list.
3. On an iOS device open the Secure Endpoint iOS connector and go to Clarity status. Select Domain Exclusions to verify the list you added.

IMPORTANT! If you modify a Clarity profile through your Meraki dashboard to add domain exclusions, these changes will be overwritten any time you make a change to the Clarity policy through your Secure Endpoint console.

Workspace ONE Domain Exclusions

To add domain exclusions in Workspace ONE you will have to download and edit a new Mobileconfig file.

1. Download the Deploy via Workspace ONE Mobileconfig file for the group you want to add exclusions to.
2. Open the Mobileconfig file in a text editor.
3. Add your domain exclusion list within the block shown in the example below. Save the file.

```
<key>VendorConfig</key>
    <dict>
        <key>affiliate_guid</key>
        <string>7e9d7d2a-b554-50f4-3ebb-d275f6f9aa30</string>
        <key>cloud_asn1_server_host</key>
        <string>cloud-ios-asn.amp.cisco.com</string>
        ...
        <key>domain_exclusions_list</key>
        <array>
            <string>www.google.com</string>
            <string>*.cisco.com</string>
            <string>www.reddit.com</string>
            <string>*.office.opendns.com</string>
        </array>
    </dict>
```

4. To update an existing profile go to **Devices > Profiles & Resources > Profiles** on your Workspace ONE dashboard.
5. Open the Clarity profile and click **Add Version**.
6. Add the modified Mobileconfig section under **Custom Settings**.

MobileIron Domain Exclusions

To add domain exclusions in MobileIron you will have to download and edit a new Mobileconfig file.

1. Download the Deploy via MobileIron Mobileconfig file for the group you want to add exclusions to.
2. Open the Mobileconfig file in a text editor.
3. Add your domain exclusion list within the block shown in the example below. Save the file.

```
<key>VendorConfig</key>
    <dict>
        <key>affiliate_guid</key>
        <string>7e9d7d2a-b554-50f4-3ebb-d275f6f9aa30</string>
        <key>cloud_asn1_server_host</key>
        <string>cloud-ios-asn.amp.cisco.com</string>
        ...
        <key>domain_exclusions_list</key>
        <array>
            <string>www.google.com</string>
            <string>*.cisco.com</string>
            <string>www.reddit.com</string>
            <string>*.office.opendns.com</string>
        </array>
    </dict>
```

4. Existing profiles in MobileIron cannot be edited so you will have to replace the existing profile with the edited Mobileconfig using the same procedure to create a Deploy via MobileIron profile.

Upgrade the Secure Endpoint iOS Connector

When an updated version of the Secure Endpoint iOS connector is available it will be pushed to the App Store and updated from there.

Uninstall the Secure Endpoint iOS Connector

See the documentation for your MDM for instructions on removing apps from managed devices.

Prevent Secure Endpoint iOS Connector Being Disabled Over Cellular Data

The iOS Settings app allows users to configure the ability to enable and disable cellular data usage on the device as a whole and for each app. If cellular data usage is

disabled for the Secure Endpoint iOS connector it is unable to provide any protection when the device is using a cellular network for data instead of wifi.

Administrators can disable access to cellular data settings through the MDM dashboard. This will prevent the user from turning off cellular data usage for the Secure Endpoint iOS connector.

IMPORTANT! Making these changes will prevent the user from turning off cellular data usage for all apps on the device.

Meraki

1. Navigate to **Profiles & settings** in the Meraki dashboard.
2. Add **Restrictions** if they have not already been added.
3. Uncheck **Allow changes to cellular data usage for apps (iOS 7+)** under **iOS restrictions (supervised)**.

MobileIron

For MobileIron you must use the Apple Configurator 2 app to modify the Clarity mobileconfig file downloaded from the Secure Endpoint or Umbrella console.

1. Open the mobileconfig file in Apple Configurator.
2. Select **Restrictions** in the left pane.
3. Uncheck **Allow modifying cellular data pp settings (supervised only)**.
4. Save the mobileconfig file and import it into your MobileIron MDM.

Workspace ONE

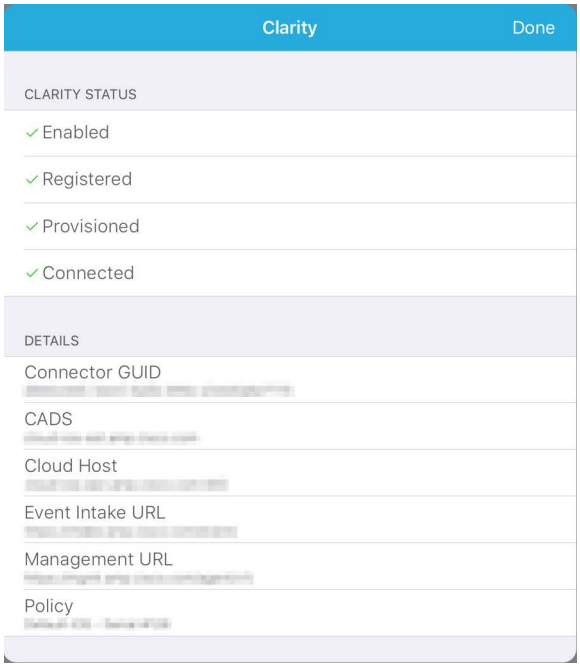
1. Navigate to **Devices > Profiles & Resources > Profiles** in the Workspace ONE dashboard.
2. Locate your Clarity or Umbrella profile and open it.
3. Click **Add Version**.
4. Uncheck **Allow changes to cellular data usage for apps** under **Restrictions**.

iOS Connector User Interface

Once the Secure Endpoint iOS app is installed on a device you can verify that Clarity and/or Umbrella are running.

1. Tap the Secure Endpoint iOS icon.

2. On the main screen, tap **Status**. A green check mark icon shows next to each component that is running.
3. Tap **Protected by Clarity** to see the Clarity status details. You can find the **connector GUID** on this screen for troubleshooting.



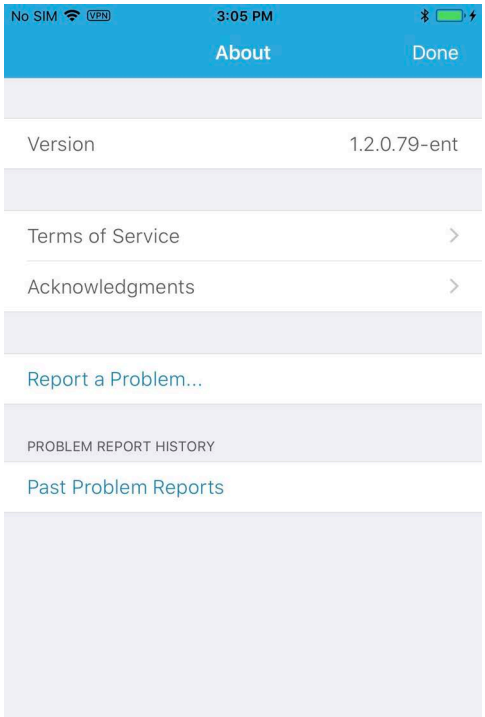
Problem Report

Users can also send problem reports from the app. The email address to send reports to is specified on the MDM Integration page.

IMPORTANT! If integrated with Umbrella, the email address for problem reports is specified in the Umbrella portal.

1. Tap the Secure Endpoint iOS icon.

2. On the main screen tap **Learn More**.
3. Tap **Report a Problem...**



4. Follow the on-screen instructions to complete the process.

Chapter 12
Secure Endpoint Android Connector

The Secure Endpoint Android connector supports Android 8.0 and higher.

You can download the app from the Google Play Store or directly from the Secure Endpoint console.

If you download the APK from the Console, it is recommended that you use a Mobile Device Manager (MDM) to push the app to the devices in your organization through a Managed Configuration.

IMPORTANT! Users who install the app through Google Play will receive connector updates depending on the Play Store app **Auto-update apps** setting.

Tap the downloaded file to begin installation.

Android Connector Firewall Exceptions

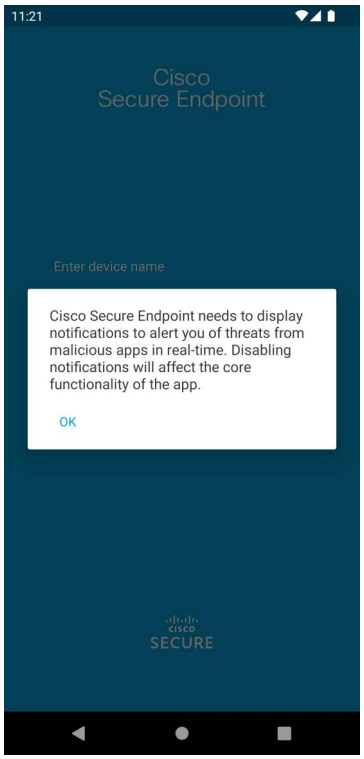
To allow the connector to communicate with Cisco systems when on wifi, the firewall must allow the clients to connect to certain servers over specific ports. Firewall exceptions for proper operation of the Secure Endpoint Android connector can be found in Connector Firewall Exceptions.

Android Installer

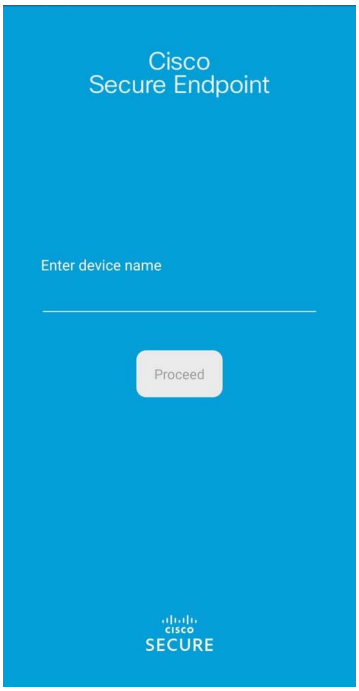
You may be prompted to review the permissions required before installation begins.

IMPORTANT! If you installed the app from Google Play you must use the activation link on your device before opening the app. Users should tap the link from email or a browser window. Do not paste the URL into the browser address bar.

1. Select Open to launch the application when the installation is complete.
2. Connector versions 2.5.0 and later running on Android 13 and later will prompt you to allow notifications. You must allow notifications to maintain the core functionality of the app to detect threats in real-time.



3. Enter a name for the device as it should be displayed in the Secure Endpoint console and tap Proceed.

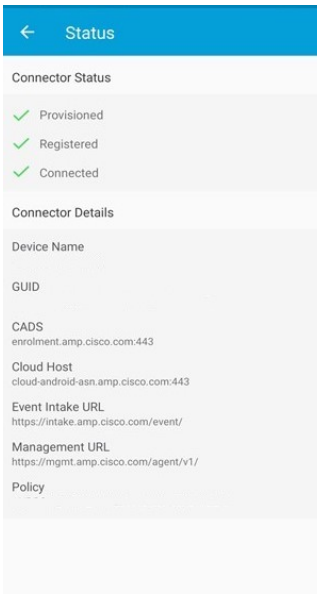


4. The Secure Endpoint Android connector will then attempt to establish a connection to the Cisco Cloud.

IMPORTANT! On a new connector install on Android 12 and higher you will need to set the connector app to open the Secure Endpoint console URLs by default. To do this, make sure to open the app after it is installed and follow the instructions in the dialog.

5. The application will begin an initial scan of the device for any malicious or non-compliant apps. After the scan is complete, tap the Summary button to view a summary of clean and malicious apps as well as any that were on the Custom Detections - Android list associated with the connector policy.

6. You can check the Status page to verify the connector is properly provisioned, registered, and connected to the Cisco cloud.



Battery Optimization

Android devices may set Battery Optimization for certain apps running in the background. If the device has enabled Battery Optimization for the Cisco Secure Endpoint app, the operating system will prevent the application from running in the background after a period of time. This will prevent real-time scanning when new apps are installed. To make sure all apps are scanned, you must disable optimization for the Cisco Secure Endpoint app in your device settings. See the documentation for your version of Android for steps to disable the setting.

Android Connector User Interface

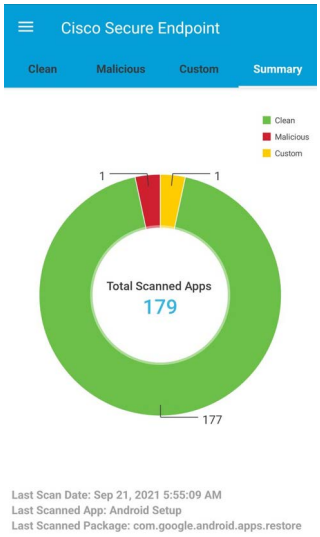
Tap the Secure Endpoint Android connector icon to launch the app.

IMPORTANT! On a new connector install on Android 12 and higher, the first time you launch the app you will be asked to set the connector app to open the Secure Endpoint console URLs by default. Follow the instructions in the dialog to continue.

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 Secure Endpoint Android app.

After a scan is completed, tap the Summary button to view a chart with 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.



Tap on the Clean tab to view a list of apps installed on the device that were clean. Tap on the Malicious tab to see the list of apps that were detected as malware. You can also use the Custom tab to see the apps from any Custom Detections - Android lists that were detected on the device. On the Malicious and Custom tabs you can also use the Uninstall button to remove the apps.

Under the tabs for clean, malicious, and custom app detections you can search for an app by name.

Retrospective detections

In cases where an app was previously thought to be clean and is later marked as malicious, a retrospective detection can be sent to the connector to move the app from the clean to malicious tab. A false-positive detection can also be moved from the malicious tab to the clean tab.

IMPORTANT! Apps can only be moved from malicious to clean if they have not already been uninstalled manually by the user.

Report a Problem

Report a problem allows the user to upload crash logs to the File Repository. If a support case needs to be opened, you can provide Cisco support with the file for troubleshooting.

Chapter 13
Connector Engines and Features

Each connector uses multiple engines and features to provide detection and response capabilities against malware, exploits, and ransomware. Settings for these are controlled through settings in Policies. Some engines and features are only available in certain versions of the connectors and will be noted.

TETRA

Available for:

- Secure Endpoint Windows connector.

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.

To enable TETRA and adjust settings go to **Advanced Settings >** TETRA in your policy.

ClamAV

Available for:

- Secure Endpoint Mac connector.
- Secure Endpoint Linux connector.

ClamAV is a full antivirus replacement and should never be enabled if another antivirus engine is installed. ClamAV can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a large environment.

To enable ClamAV and adjust settings go to Advanced Settings > **ClamAV** in your policy.

Exploit Prevention

Available for:

- Secure Endpoint Windows connector 6.0.5 and later.

The exploit prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine. You can use Device Trajectory to help determine the vector of the attack and add it to a Custom Detections - Simple list.

To enable the exploit prevention engine, go to Modes and Engines in your policy and select audit or block mode. Audit mode is only available on Secure Endpoint Windows connector 7.3.1 and later. Earlier versions of the connector will treat audit mode the same as block mode.

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

Protected Processes

The exploit prevention engine protects the following 32-bit and 64-bit (Secure Endpoint Windows connector version 6.2.1 and higher) processes and their child processes:

- Microsoft Excel Application
- Microsoft Word Application
- Microsoft PowerPoint Application
- Microsoft Outlook Application
- Internet Explorer Browser
- Mozilla Firefox Browser
- Google Chrome Browser
- Microsoft Skype Application
- TeamViewer Application
- VLC Media player Application
- Microsoft Windows Script Host
- Microsoft Powershell Application
- Adobe Acrobat Reader Application
- Microsoft Register Server
- Microsoft Task Scheduler Engine
- Microsoft Run DLL Command
- Microsoft HTML Application Host
- Windows Script Host
- Microsoft Assembly Registration Tool
- Zoom
- Slack

- Cisco Webex Teams
- Microsoft Teams

You can exclude any applications from exploit prevention protection by adding Executable Exclusions for Exploit Prevention.

IMPORTANT! If you disable exploit prevention you will have to restart any of the protected processes listed above that were running.

It also monitors the following directories:

- Windows AppData Temp Directory (\Users\[username]\AppData\Local\Temp\)
- Windows AppData Roaming Directory (\Users\[username]\AppData\Roaming\)

Exploit prevention protects processes it does not normally protect from injection attempts by any applications launched from those directories.

Excluded Processes

The following processes are excluded from exploit prevention monitoring because of compatibility issues:

- McAfee DLP Service
- McAfee Endpoint Security Utility

Exploit prevention version 5

Available for:

- Secure Endpoint Windows connector 7.5.1 and later.

Secure Endpoint Windows connector 7.5.1 includes a significant update to exploit prevention. New features in this version include:

- Protect network drives – Automatically protects processes running from network drives against threats like ransomware.
- Protect remote processes – Automatically protects processes running remotely on protected computers using a domain authenticated user (admin). The protection includes only processes created with one of these tokens: Kerberos, NtLmSsp or Schannel (e.g. psexec). Processes in the exclusion list are also excluded from remote execution protection.
- AppControl bypass through rundll32 – Stops specially crafted rundll32 command lines that allow running interpreted commands.
- UAC bypass – Blocks privilege escalation by malicious processes by preventing Windows User Account Control mechanism bypasses.
- Browser/Mimikatz vaults credential – If enabled, exploit prevention will protect against credential theft in Microsoft Internet Explorer and Edge browsers.
- Shadow copy deletion – Traces the deletion of shadow copies by intercepting the COM API in the Microsoft Volume Shadow Copy Service (vssvc.exe). Deletion of shadow copies commonly precedes a ransomware attack. Exploit prevention will produce a threat log when a shadow copy is deleted. It will detect the deletion of shadow copies but will not block the deletion.

- SAM hashes – Protects against SAM hash credential theft by Mimikatz by intercepting attempts to enumerate and decrypt all the SAM hashes in the registry hive `Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users`. Adversaries may attempt to dump credentials to obtain account login and credential details (usually in the form of a hash or a clear text password) from the operating system and software.
- Protect running processes – Inject into running processes, if those have started before the exploit prevention instance (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe).

These features are all enabled by default when exploit prevention is enabled in policy.

Script Control

Available for:

- Secure Endpoint Windows connector 7.3.1 and later.

Script control allows the exploit prevention engine to prevent certain DLLs from being loaded by some applications and their child processes. The engine will kill a process if it or one of its child processes listed below attempts to load one of the blocked DLLs.

Processes	Child Processes	Blocked DLLs
winword.exe excel.exe powerpnt.exe outlook.exe	cscript.exe wscript.exe powershell.exe mshta.exe cmd.exe rundll32.exe regsvr32.exe autoit3.exe cmstp.exe node.exe	wbemdisp.dll System.Management.Automation.dll System.Management.Automation.ni.dll
regsvr32.exe	cscript.exe wscript.exe powershell.exe mshta.exe cmd.exe rundll32.exe regsvr32.exe autoit3.exe cmstp.exe node.exe	scrobj.dll

Incompatible Software

The exploit prevention engine is incompatible with the following software:

- Malwarebytes
- F-Secure DeepGuard

- ByteFence
- Microsoft Enhanced Mitigation Experience Toolkit (EMET)

IMPORTANT! See this Secure Endpoint TechNote for instructions how to manage EMET compatibility.

There is also a known issue with Sophos Endpoint Protection that causes MS Word 2016 to fail to exit properly when you close the application.

System Process Protection

Available for:

- Secure Endpoint Windows connector 6.0.5 and later.

The system process protection engine protects critical Windows system processes from being compromised through memory injection attacks by other processes.

To enable system process protection, go to Modes and Engines in your policy and choose protect or audit from the system process protection conviction mode.

Protected System Processes

System process protection protects the following processes:

- Session Manager Subsystem (smss.exe)
- Client/Server Runtime Subsystem (csrss.exe)
- Local Security Authority Subsystem (lsass.exe)
- Windows Logon Application (winlogon.exe)
- Windows Start-up Application (wininit.exe)

Malicious Activity Protection

Available for:

- Secure Endpoint Windows connector 6.1.5 and later.

The malicious activity protection engine defends your endpoints from ransomware attacks by identifying malicious actions of processes when they execute and stops them from encrypting your data. Because the malicious activity protection engine detects threats by observing the behavior of running processes, it can determine if a system is under attack by a new variant of ransomware that may have eluded other security products and detection technology.

To enable the malicious activity protection engine, go to Modes and Engines in your policy and choose audit, block, or quarantine from malicious activity protection

conviction mode. The malicious activity protection engine is not currently compatible with Hyper-V clusters.

IMPORTANT! While the connector will be able to detect and prevent ransomware from completely compromising your data, some files will be encrypted by the attack before the connector can determine that the process meets its criteria for being labeled as ransomware. Unfortunately, it may be impossible to decrypt these files. However, the connector will report the first 5 files that were modified by the offending process so that you can easily restore them from backups if necessary. However, please note that it is possible for more files to be encrypted in the time from when the connector detects the process as being malicious and when it is able to successfully block/quarantine the process.

Endpoint Isolation

Available for:

- Secure Endpoint Windows connector 7.0.5 and later.
- Secure Endpoint Mac connector 1.21.0 and later.

Endpoint isolation is a feature that lets you block incoming and outgoing network activity on a Windows computer to prevent threats such as data exfiltration and malware propagation. It is available on 64-bit versions of Windows that support version 7.0.5 and later of the connector.

Endpoint isolation sessions do not affect communication between the Windows connector and the Cisco cloud. There is the same level of protection and visibility on your endpoints as before the session. You can configure IP Isolation Allow Lists of addresses that the connector will not block during an active endpoint isolation session.

Start an Endpoint Isolation Session

Isolating an endpoint blocks all network traffic except for communication to the Cisco cloud and any other IP addresses configured in your IP isolation allow list.

To start an endpoint isolation session:

1. In the console, navigate to Management > Computers.
2. Locate the computer you want to isolate and click to display details.
3. Click the Start Isolation button.

The connector user interface will indicate that the endpoint is isolated.

IMPORTANT! For Secure Endpoint Mac connector only – any cached browser content will be available but browser connections will be halted. Note that the Mac connector can also be uninstalled during an isolation session.

Stop an Endpoint Isolation Session

Stopping an isolation session restores all network traffic to an endpoint.

To stop an endpoint isolation session from the console:

1. In the console, navigate to Management > Computers.
2. Locate the computer you want to stop isolating and click to display details.
3. Click the Stop Isolation button.
4. Enter any comments about why you stopped isolating the endpoint.

The connector user interface will indicate that the endpoint isolation session has ended.

Stop a Windows Isolation Session From the Command Line

If an isolated endpoint loses its connection to the Cisco cloud, it will not be possible to stop the isolation session from the console. In these situations, you can stop the session locally from the command line.

To stop an endpoint isolation session from the command line

1. In the console, navigate to Management > Computers.
2. Locate the computer you want to stop isolating and click to display details.
3. Note the unlock code.
4. Open a command prompt with administrator privileges on the isolated computer.
5. Navigate to the directory where the connector is installed (C:\Program Files\Cisco\AMP\[version number]) and execute `sfc.exe -n [unlock code]`

IMPORTANT! If you enter the unlock code incorrectly 5 times you will not be able to make another unlock attempt for 30 minutes.

The connector user interface will indicate that the endpoint isolation session has ended.

IMPORTANT! If there is an active isolation session in progress, some connector behavior will be blocked:
- Updating the policy to turn off the feature (not to be confused with stopping the isolation session). Policy updates that do not turn off the feature will be allowed.
- Uninstalling the connector. If you attempt to uninstall the connector during an active isolation session, it will exit with code 16010.
- Upgrading the connector. If you attempt to upgrade the connector while it is isolated, there will be a product update failed message in the console events.

Stop a macOS Isolation Session From the Command Line

If an isolated endpoint loses its connection to the Cisco cloud, it will not be possible to stop the isolation session from the console. In these situations, you can stop the session locally from the command line.

To stop an endpoint isolation session from the command line

1. In the console, navigate to Management > Computers.
2. Locate the computer you want to stop isolating and click to display details.

3. Note the unlock code.
4. Open a terminal on the isolated computer.
5. Navigate to the directory where the connector is installed (/opt/cisco/amp) and execute `./ampcli isolate stop [unlock code]`

IMPORTANT! If you enter the unlock code incorrectly 5 times you will not be able to make another unlock attempt for 30 minutes.

The connector user interface will indicate that the endpoint isolation session has ended.

IMPORTANT! If there is an active isolation session in progress, some connector behavior will be blocked:
- Updating the policy to turn off the feature (not to be confused with stopping the isolation session). Policy updates that do not turn off the feature will be allowed.
- Upgrading the connector. If you attempt to upgrade the connector while it is isolated, there will be a product update failed message in the console events.

Orbital

IMPORTANT! Orbital is available for customers with Secure Endpoint advantage package or higher.

Available for:

- Secure Endpoint Windows connector 7.1.5 and later.
- Secure Endpoint Mac connector 1.16.0 and later.
- Secure Endpoint Linux connector 1.17.0 and later.

Orbital is a Cisco service that can be deployed on your endpoints then used by Secure Endpoint to query endpoints for detailed information. Orbital can execute queries immediately, or you can schedule them using the Orbital jobs feature.

For details on using Orbital, see the Orbital documentation at https://orbital.amp.cisco.com/help/.

Orbital Windows Requirements

Orbital requires Windows 10 1709 and later or Windows Server 2012, 2012 R2, 2016 and later. It is available for Secure Endpoint Windows connector version 7.1.5 and later.

Known Issue/Limitation

The Orbital process is not protected by the connector even when the connector protection feature is enabled. This means that users with suitable permissions can stop or uninstall the Orbital service. The Windows connector will reinstall Orbital the next time the update interval is reached.

Orbital macOS Requirements

Orbital requires macOS 10.15 and later. It is available for Secure Endpoint Mac connector version 1.16.0 and later on Intel processors, or 1.20.0 and later on Apple silicon (requires Orbital Node 1.21.0 or later).

Grant Full Disk Access

Orbital requires full disk access on macOS to perform queries.

If you're using a Mobile Device Management (MDM) solution (e.g. Cisco Meraki) for deployment and management, full disk access can be granted using the Privacy Preferences Policy Control Payload in an MDM profile. This removes the need for action by the end-user. For Secure Endpoint Mac connector 1.14.0 and later see Advisory for Secure Endpoint Mac Connector on macOS 11 (Big Sur), macOS 10.15 (Catalina, and macOS10.14 (Mojave).

The user will have to accept the MDM profile on Macs running macOS 10.13.4 and later if they are not in the Device Enrollment Program (DEP).

Use the following steps if you're not using an MDM:

1. Launch System Preferences.
2. Click Security and Privacy.
3. Click the lock to make changes.
4. Select Full Disk Access from the left pane and add `/Library/Application/ Support/Cisco/AMP for Endpoints Connector/Orbital/Cisco Orbital.app` by doing the following:

Click the + button and choose `/Library/Application/ Support/Cisco/AMP for Endpoints Connector/Orbital/Cisco Orbital.app` in the file selector dialog.

Enable Orbital in a Policy

Secure Endpoint can deploy Orbital automatically if your endpoints already have a connector installed. Orbital is bundled with the Secure Endpoint Windows and Mac connector packages for deployment when you enable it in a policy. For details, see Orbital.

You can force an Orbital update in Secure Endpoint Windows connector version 7.4.5 and higher using the following command from the connector install directory using an account with administrator permission:

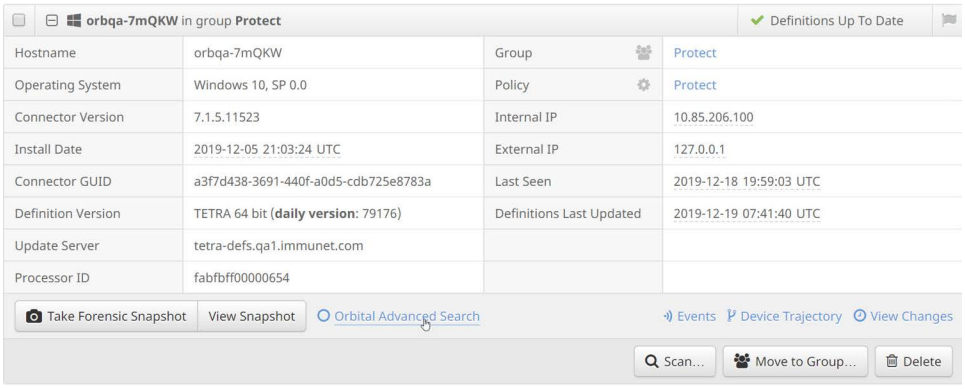
```
sfc.exe -forceOrbitalUpdate
```

This command will remove any cached versions that failed and retry the current version.

Access Orbital from the Secure Endpoint console

You can access Orbital from the Secure Endpoint console in a couple of ways. Select **Analysis > Orbital Advanced Search** to go directly to the Orbital console.

To access Orbital for a specific computer, go to **Management > Computers** and locate the computer you want to search. Click the **Orbital Advanced Search** link for the computer.



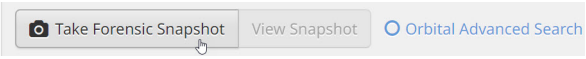
This takes you to the Orbital console where you can run queries on the computer. The computer's GUID is automatically populated in the Endpoints field in the Orbital console.

For information on running queries in Orbital, see the Quick Start section of the Orbital documentation at https://orbital.amp.cisco.com/help/quick-start/.

Forensic Snapshot

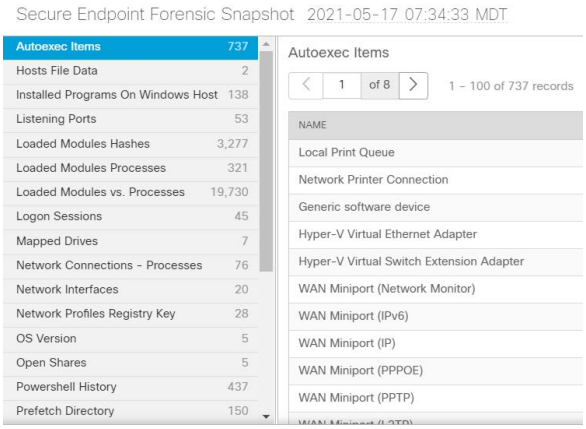
You can use Orbital to take a forensic snapshot of a computer. A forensic snapshot is a preconfigured set of queries that gathers forensically relevant information about the current state of the endpoint, including running processes, loaded modules, autorun executables, and so on.

To access the forensic snapshot feature, go to **Management > Computers** and locate the computer you want to search. Click the **Take Forensic Snapshot** button.

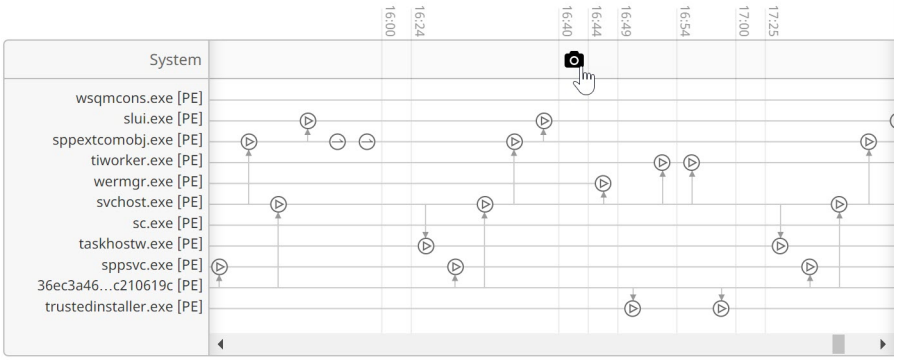


IMPORTANT! Some Behavioral Protection signatures can automatically trigger a forensic snapshot on the endpoint.

The request is sent to the endpoint. Once the snapshot is complete, click **View Snapshot** to see the results.



You can also access the forensic snapshot results from the computer's device trajectory page.



Script Protection

Available for:

- Secure Endpoint Windows connector 7.2.1 and later.

The script protection feature provides visibility into scripts executing on your endpoints and helps protect against script-based attacks commonly used by malware. Script protection provides additional visibility into the execution chain of scripts in Device Trajectory so that you can observe which applications are attempting to execute scripts on your endpoints. Script protection requires Windows 10 version 1709 and later or Windows Server 2016 version 1709 and later.

To enable script protection, go to modes and engines in your policy and choose audit or quarantine from the script protection conviction mode. Script protection is not

dependent on TETRA but if TETRA is enabled script protection will use it to provide additional protection.

IMPORTANT! When running in quarantine mode script protection has the potential to impact user applications such as Word, Excel, and Powerpoint. If these applications attempt to execute a malicious VBA script, the application will be stopped.

Script protection works with the following script interpreters:

- PowerShell (V3 and later)
- Windows Script Host (wscript.exe and cscript.exe)
- JavaScript (non-browser)
- VBScript
- Office VBA macros

IMPORTANT! Script protection does not provide visibility nor protection from non-Microsoft script interpreters such as Python, Perl, PHP, or Ruby.

Script protection provides protection from fileless malware by leveraging the same analysis engine as behavioral protection (connector version 7.5.1 and later). It analyzes parts of scripts that are executing (buffers) and comparing them to malicious script signatures that are updated regularly. Scripts with malicious content detected will be blocked from executing.

Behavioral Protection

Available for:

- Secure Endpoint Windows connector 7.3.1 and later.
- Secure Endpoint Linux connector 1.22.0 and later

The behavioral protection engine enhances the ability to detect and stop threats behaviorally. It deepens the ability to detect "living-off-the-land" attacks and provides faster response to changes in the threat landscape through signature updates. It is available on 64-bit versions of Windows supported by version 7.3.1 and later of the connector.

The engine can take the following actions when malicious activity is detected:

- End processes.
- Quarantine files.
- Upload files for analysis.
- End process trees.
- Trigger a Forensic Snapshot for certain detections when Orbital Advanced Search is also enabled.

Behavioral Protection monitors the following system activity:

- Processes.
- File events.

- Registry events.
- Network events.

IMPORTANT! Behavioral protection cannot monitor network events if network is set to disabled in Modes and Engines or the connector was installed using the /skipdfc switch.

Additional Requirements for Windows

Behavioral protection also requires a CPU that supports the Supplemental Streaming SIMD Extensions 3 (SSSE3) instruction set. See your CPU manufacturer's documentation for a list of processors that includes SSSE3. A signature set update failure with error code 50 will be in your events list if the processor on a computer does not support SSSE3.

IMPORTANT! Some virtualization technologies, including Hyper-V and VMware, have settings that can mask SSSE3 capabilities in the virtual machine even if the host CPU supports them. See your virtual machine documentation to ensure these settings are disabled to use behavioral protection.

Additional Requirements for Linux

Behavioral Protection is available on distributions listed with these minimum kernel versions or later.

Behavioral Protection Kernel Versions

Linux Distribution	Minimum Kernel Version
Oracle	3.10.0-940
RHEL/CentOS	3.10.0-940
AlmaLinux/Rocky Linux	4.18.0
Amazon Linux 2	4.18.0
SUSE	4.18.0
Debian	4.18.0
Ubuntu	4.18.0

Remote Uninstall

Available for:

- Secure Endpoint Windows connector.

  IMPORTANT! Note that Cisco Secure Client deployed through Cloud Management on Cisco XDR or SecureX is not currently supported.

- Secure Endpoint Mac connector.
- Secure Endpoint Linux connector.

Secure Endpoint administrators can uninstall connectors from endpoints with this feature. Navigate to Management -> Computers and locate the endpoint you want to uninstall. Expand the computer pane and click Uninstall Connector. The endpoint will be removed from the Computers list and an audit log entry and event will be created. This is a full uninstall and will delete the connector history and any files in quarantine.

IMPORTANT! Isolated connectors cannot be uninstalled and the uninstall button will be unavailable for these endpoints. End the isolation session then the uninstall button will be available.

The user will not need to enter a password to uninstall the Secure Endpoint Windows connector if Connector Protection is enabled under Administrative Features in the policy. A reboot is not required on Windows unless you plan to re-install a connector on the endpoint. No reboot is required for Mac or Linux.

The user will be prompted to enter an administrator password to uninstall the Secure Endpoint Mac connector on unmanaged versions of macOS prior to version 12.0. The uninstall will fail if the user does not enter the administrator password. See Configure Permissions for Secure Endpoint Mac Connector and Orbital with MDM: Full Disk Access, System Extensions for further details.

Chapter 14
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 observables 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 Secure Endpoint 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 Secure Endpoint 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 Secure Endpoint 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.

Run Scan On is the date and time the scan should begin. The time corresponds to the local time on the computer the Secure Endpoint 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 Secure Endpoint Windows 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 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 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 Secure Endpoint 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 Secure Endpoint Dashboard.

Chapter 15
Automated Actions

The Automated Actions page lets you set actions that automatically trigger when a specified event occurs on a computer. You can access the page from **Outbreak Control > Automated Actions** on the main menu.

IMPORTANT! Automated Actions can only run actions on connectors which support the action. For connectors or operating systems that do not meet the minimum requirements, or for which the desired features are not enabled in policy, the automated action will not be triggered.

Automated Actions Tab

The Automated Actions tab allows you to adjust the settings on each action and set them to active or inactive.

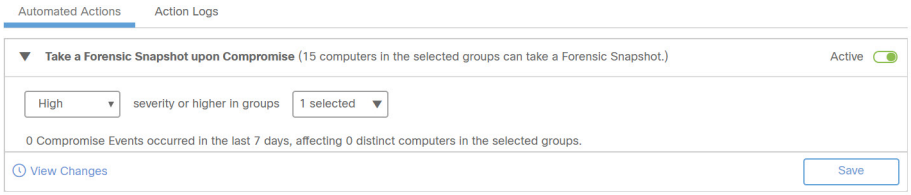
Automated actions do not occur in a set order. Some automated actions may execute before others even if a trigger event satisfies the conditions on multiple actions. For example, a computer that was isolated cannot be moved to a different group while it is isolated.

Forensic Snapshot Automated Action

IMPORTANT! The Forensic Snapshot Automated Action is available for customers with Secure Endpoint Advantage. Orbital Advanced Search must be enabled on your endpoint to take a Forensic Snapshot. See the Orbital Windows Requirements and Orbital macOS Requirements.

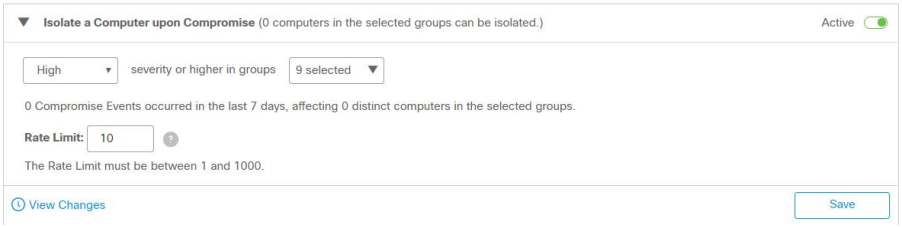
You can set an Automated Action to take a Forensic Snapshot of a computer when a compromise occurs.

To enable the Automated Action, first select the severity of compromise. Events that are the selected severity or higher will trigger the automated action. Next, set the group(s) you want the action to apply to, then click **Save**. Once an action has been created, set it to Active or Inactive.



Endpoint Isolation Automated Action

You can set an Automated Action to isolate computers when a compromise occurs. Isolation is supported on Windows connector 7.0.5 and later and Mac connector 1.21.0 and later.



To enable the Automated Action, first select the severity of compromise. Events that are the selected severity or higher will trigger the automated action. Next, set the group(s) you want the action to apply to, and set a Rate Limit for the number of computers you want to allow to be isolated (the maximum is 1000). Click **Save** to create your action. Once an action has been created, set it to Active or Inactive.

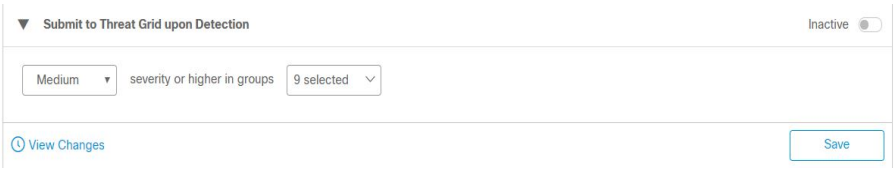
The Rate Limit protects you against false positive detections. The Rate Limit feature looks at the total number of isolations in a 24 hour rolling window. If the number of isolations is greater than the limit, no further isolations are triggered. Computers will be isolated again once the number of compromise events falls to fewer than the limit in the 24 hour rolling window or you stop isolation on computers that were automatically isolated.

IMPORTANT! The number of endpoints in your organization, the frequency of compromises, and your tolerance for false positives are all factors you should consider when choosing a Rate Limit. We recommend you begin with a small number.

For information on bulk stopping isolations, see Action Logs Tab.

Submit to Secure Malware Analytics Automated Action

You can set an Automated Action to submit a file to Secure Malware Analytics for File Analysis when a detection occurs.



To enable the Automated Action, first select the severity of compromise. Events that are the selected severity or higher will trigger the automated action. Next, set the group(s) you want the action to apply to. Click **Save** to create your action. Once an action has been created, set it to Active or Inactive.

Files will not be sent for analysis through the automated action if there is a corresponding quarantine event, the event was marked as resolved on the Inbox Tab, or is determined to be a false positive. Also, files that have already been submitted for analysis by your organization will not be submitted again.

The number of files that can be submitted for analysis is governed by your **Daily submissions for Automatic Analysis** setting under Secure Malware Analytics API in your Organization Settings. The files will be analyzed using the operating system specified in **VM image for analysis**.

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. Files should not be password protected.

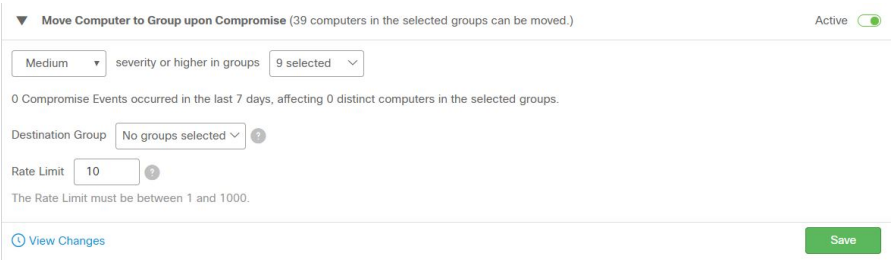
IMPORTANT! If the file was quarantined by another AV product on the computer it cannot be submitted for analysis through Automated Actions. You will need to retrieve the file from the AV product's quarantine location and submit the file manually through the File Analysis Landing Page.

Once the file analysis is complete, the analysis report will be available on the File Analysis Landing Page. You will need to have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication enabled to view the analysis.

Move to Group Automated Action

The Move to Group action will move computers from their current groups to another group when the action is triggered. This allows you to move compromised computers

to a group with a policy that has more aggressive scanning and engine settings to remediate the compromise.



To enable the Automated Action, first select the severity of compromise. Events that are the selected severity or higher will trigger the automated action. Next, set the group(s) you want the action to apply to and the destination group, and set a Rate Limit for the number of computers you want to allow to be moved (the maximum is 1000). Click **Save** to create your action. Once an action has been created, set it to Active or Inactive.

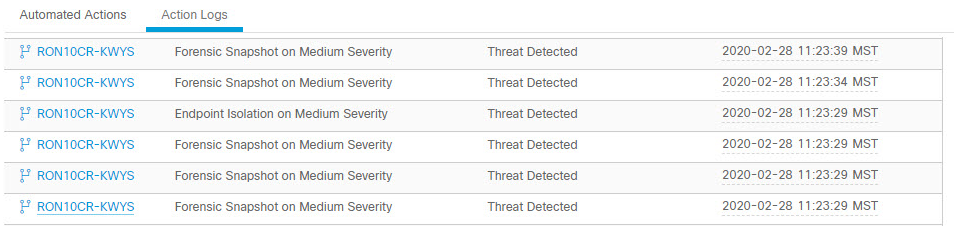
IMPORTANT! Make sure if you move computers that are included in other actions that the destination group has other features like Endpoint Isolation enabled and the group is included in your other actions.

The Rate Limit protects you against false positive detections. The Rate Limit feature looks at the total number of group moves in a 24 hour rolling window. If the number of moves is greater than the limit, no further moves are triggered. Computers will be moved again once the number of compromise events falls to fewer than the limit in the 24 hour rolling window.

IMPORTANT! The number of endpoints in your organization, the frequency of compromises, and your tolerance for false positives are all factors you should consider when choosing a Rate Limit. We recommend you begin with a small number.

Action Logs Tab

The **Action Logs** tab shows you which Automated Actions were triggered, on which computers, and when. Select the computer to go to its Device Trajectory page.



The Action Logs tab includes a button to **Stop All Isolations**. You may want to use this if there was a false positive or all incidents have been resolved. When you click the button, Secure Endpoint attempts to stop isolation on all connectors that have been isolated through Automated Actions or that are pending isolation through Automated Actions. You may need to temporarily adjust or disable the Endpoint Isolation

Automated Action to prevent it from triggering again if the issues that originally triggered it have not been resolved.

CHAPTER 16
SEARCH

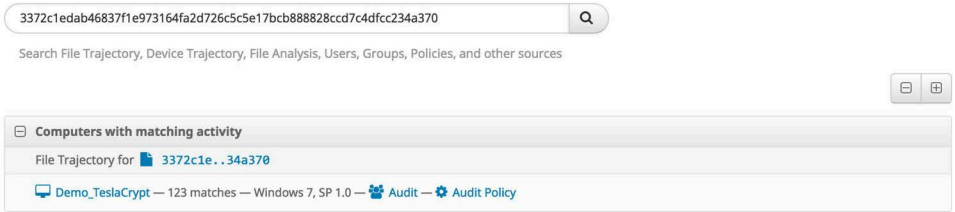
Search allows you to find information from your Secure Endpoint deployment. You can search by terms like file, hostname, URL, IP address, device name, user name, policy name and other terms. The searches will return results from File Trajectory, Device Trajectory, File Analysis and other sources. To access Search you can navigate through **Analysis > Search** or right-click various elements in the Secure Endpoint 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 connectors that observed the file.



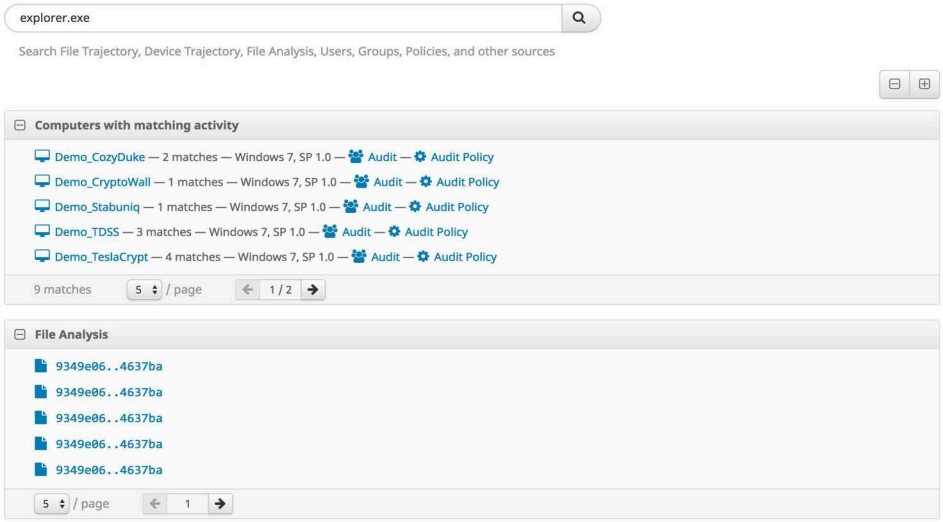
String Search

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
- Secure Endpoint policy names
- Secure Endpoint group names
- Device names (prefix match only)
- Device serial numbers (iOS devices)
- Indications of Compromise names, descriptions, tactics, or techniques

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 Secure Endpoint deployment.

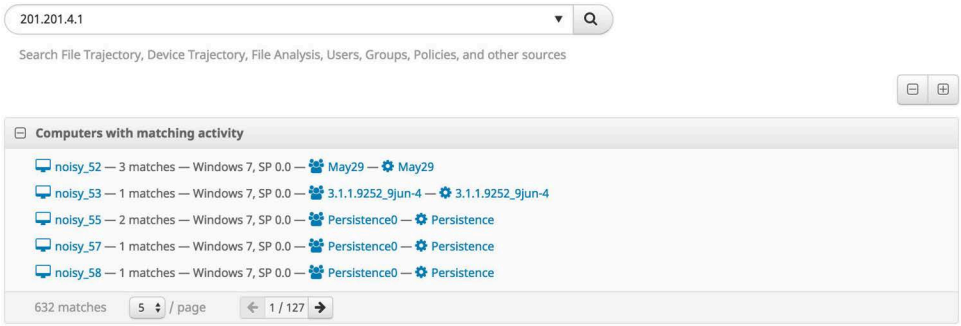


Network Activity Searches

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

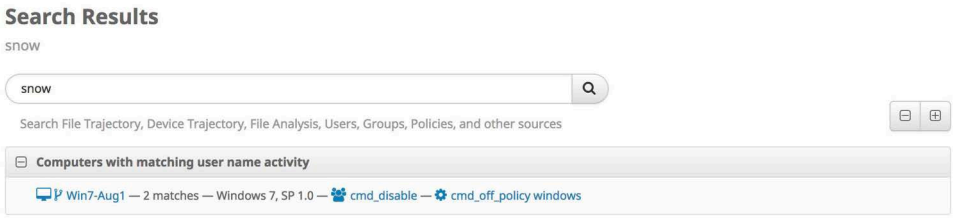
IP address searches must be exact and use the full 32 bits in dot-decimal notation. IP address search results can include devices that have contacted that address or that have observed that IP.

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



User Name Search

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 organization 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 17
File Analysis

File Analysis allows a Secure Endpoint 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 Secure Malware Analytics (formerly 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 Secure Malware Analytics 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 Secure Malware Analytics; 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 Secure Malware Analytics API key on the Organization Settings 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. Files should not be password protected.

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.

Analysis Report

ID	31a15d41803231df445cbe1978553085
OS	2600.xpsp.080413-2111
Started	12/26/14 18:08:00
Ended	12/26/14 18:14:14
Duration	0:06:14
Sandbox	bubonia (pilot-d)
Filename	0b384dc42e8d31e515739e30e3e5600d9546b0941f151daec8aba4ac5cb674b8.exe
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Analyzed As	exe
SHA256	0b384dc42e8d31e515739e30e3e5600d9546b0941f151daec8aba4ac5cb674b8
SHA1	4d70fde118949a6cf268658382f8b7b6875ed549
MD5	f09d1e4f5c5d97128ef68e2c71c218ad

Warnings

Executable Failed Integrity Check

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 Secure Malware Analytics 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 Secure Malware Analytics analysis. These indicators quickly explain any behaviors that might indicate malicious or suspicious activity. Secure Malware Analytics 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.

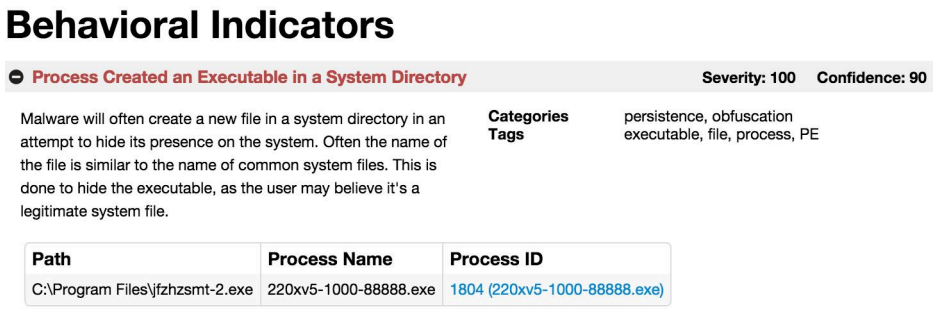
Behavioral indicators are listed in order by priority according to their potential severity (with most severe threats listed first), which is reflected by the color coding:

- 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.

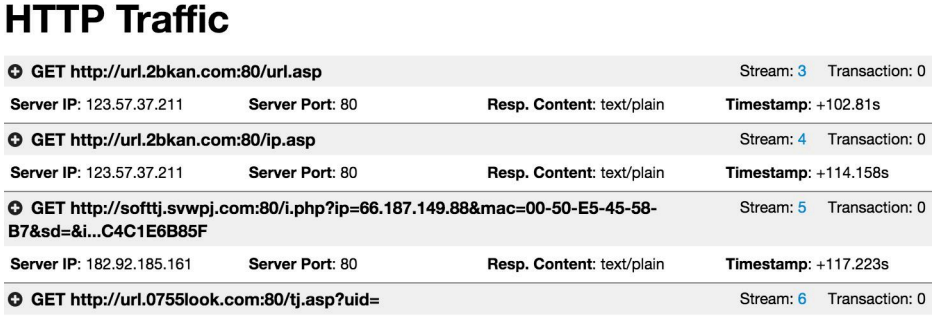
Path – The full path of any files created or modified during execution.

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

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

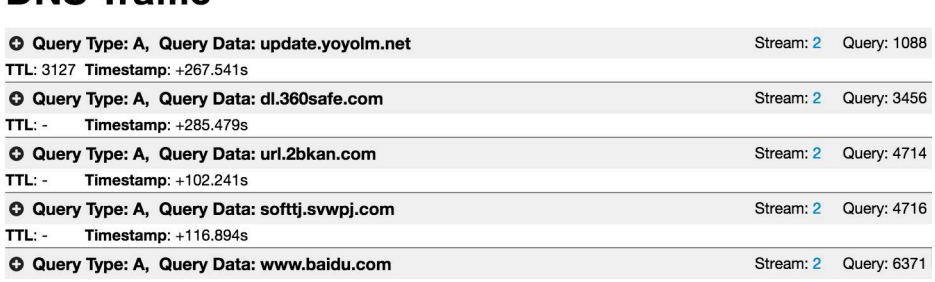
HTTP Traffic

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

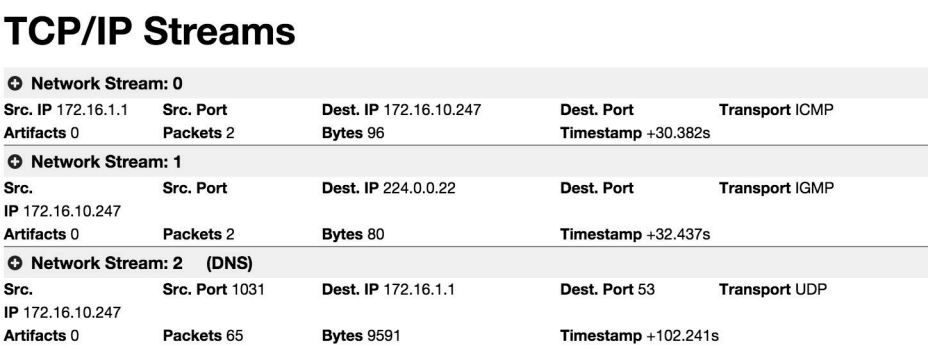


TCP/IP Streams

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 Secure Malware Analytics during analysis.

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

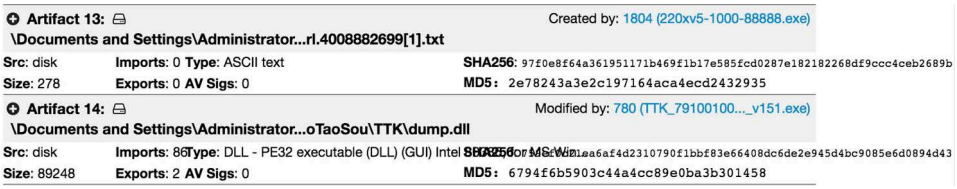


Processes

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

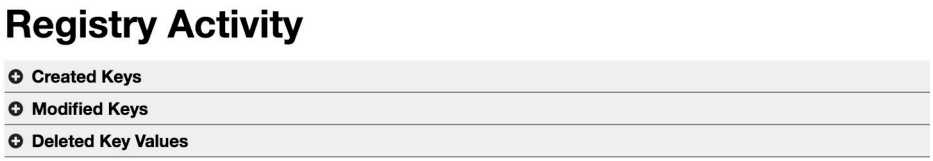
Artifacts

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



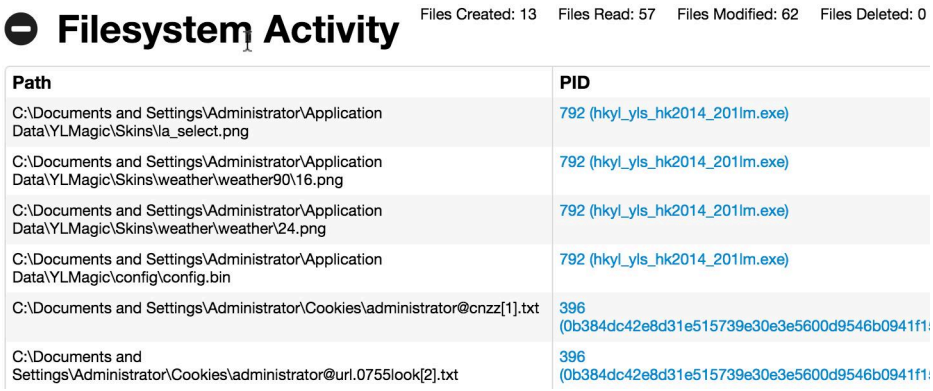
Registry Activity

If analysis detects changes to the registry, Secure Malware Analytics 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, Secure Malware Analytics 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 18
Trajectory

Trajectory shows you activity within your Secure Endpoint deployment, either across multiple computers or on a single computer or device.

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.

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:

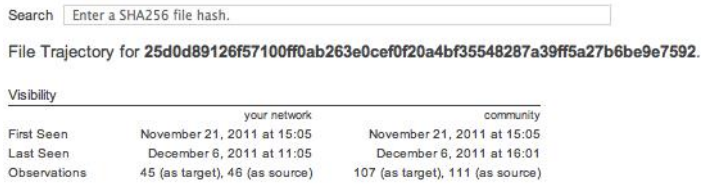
- Clean files: 7 days
- Unknown files: 1 hour
- Malicious files: 1 hour

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

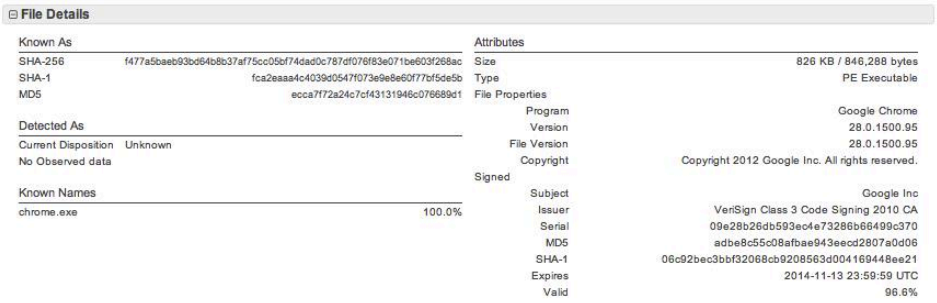
Visibility includes the First Seen and Last Seen dates and the total number of observations of the file in question in your network. Observations shows the number of times that the file in question was both a source of activity and when it was a target of activity. Note that the number of observations 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 Secure Endpoint 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.

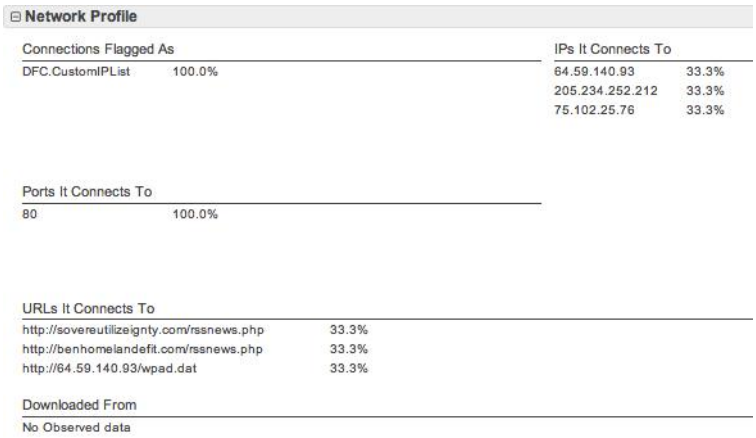


- Known As shows the SHA-256, SHA-1, and MD5 hash of the file.
- Attributes displays the file size and type.
- Known Names includes any names the file went by on your network.
- Detected As shows any detection names in the case of a malicious file.

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

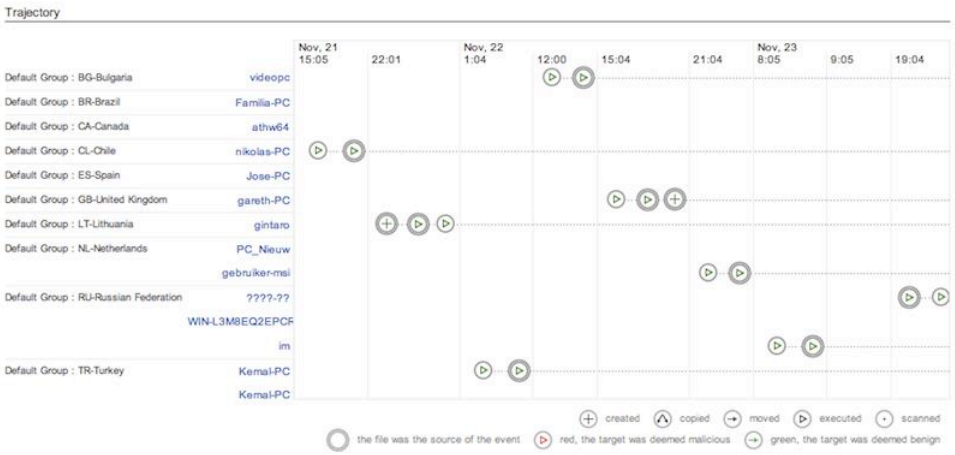
Network Profile shows any network activity the file may have participated in. If there are no entries in this section, this does not necessarily mean the file is not capable of it, but your connectors did not observe it participating in any while it was in your

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 blocked list 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 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.

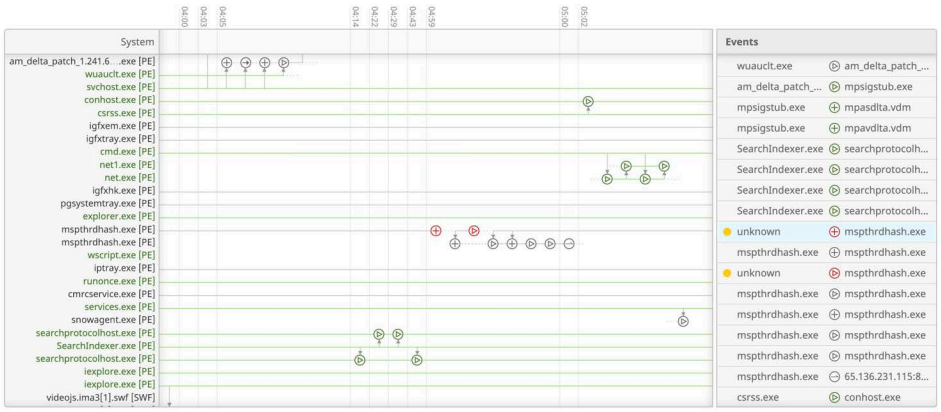
Device Trajectory is capable of storing 30 days of file events in your environment. When a file triggers an event the file is cached for a period of time before it will trigger another event. The cache time is dependent on the disposition of the file:

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

Device Trajectory displays the following file types:

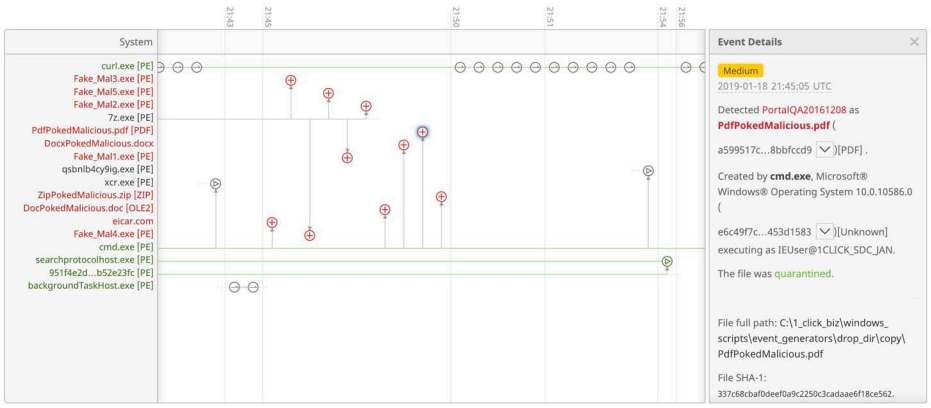
- Executable files
- Portable Document Format (PDF) files
- MS Cabinet files
- MS Office files
- Archive files
- Adobe Shockwave Flash
- Plain text files
- Rich text files
- Script files
- Installer files

The vertical axis of the Device Trajectory shows a list of files and processes observed on the computer by the connector and the horizontal axis represents the time. Running processes are represented by a solid horizontal line with child processes and files the process acted upon stemming from the line. A list of file events is displayed on the right side of the device trajectory.



IMPORTANT! If the selected row is off-screen, click ⌃ or ⌄ to return to it.

Click on an event to view its details.



Event details 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. Click if you scroll away from the selected event in the pane to return to the event.

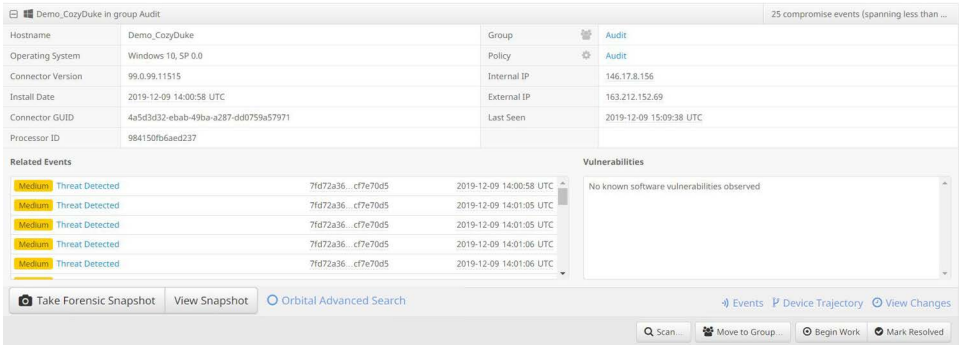
IMPORTANT! For descriptions of threat names, see AMP Naming Conventions.

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.

Secure Endpoint 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 view details of the selected computer from the Device Trajectory view by clicking on the computer name in the Device Trajectory view.

IMPORTANT! You can copy and share a URL of the current Device Trajectory view with other users in your organization by clicking the Share button then clicking Copy URL.

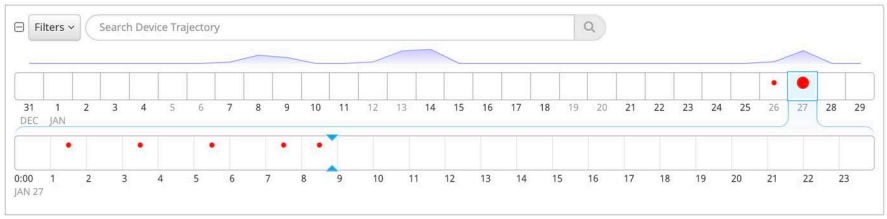


You can also perform several actions on the computer from here, such as: run a full or flash scan, move the computer to a different group, or initiate diagnostics (see Computer Management: Connector Diagnostics).

IMPORTANT! Click the fullscreen button to expand the Device Trajectory view to fill the entire screen. Click the button again to return to the normal view.

The Navigator

The navigator enables you to quickly locate and pinpoint events in the Device Trajectory. The upper ribbon displays the last 30 days, and the miniature line graph above it represents the level of activity on the computer over this period. Red dots on the 30-day ribbon represent the occurrence of compromise events. Search results appear as blue dots. The size of the dots are relative to the number of events per day. Below the 30-day ribbon is the 24-hour ribbon, which represents the 24 hours of the selected day.



Clicking on the 30-day ribbon navigates to the corresponding day in the Device Trajectory and displays the day's events in the 24-hour ribbon. You can click on the 24-hour ribbon to center the Device Trajectory on the desired time.

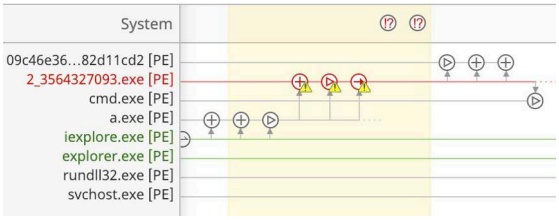
You can collapse the navigator by clicking the - button and expand it again by clicking on the ribbon or the + button.

IMPORTANT! You can hover over dots to display the number of events that they represent.

Trajectory Indications of Compromise

When certain series of events are observed on a single computer, they are seen by Secure Endpoint as indications of compromise. In Device Trajectory, these events will be highlighted yellow so they are readily visible. There will also be a separate compromise event in the Trajectory that describes the type of compromise. Clicking on the compromise event will also highlight the individual events that triggered it with

a blue halo. A description of the indicator and the tactics and techniques will also be displayed in the Event Details pane of the trajectory



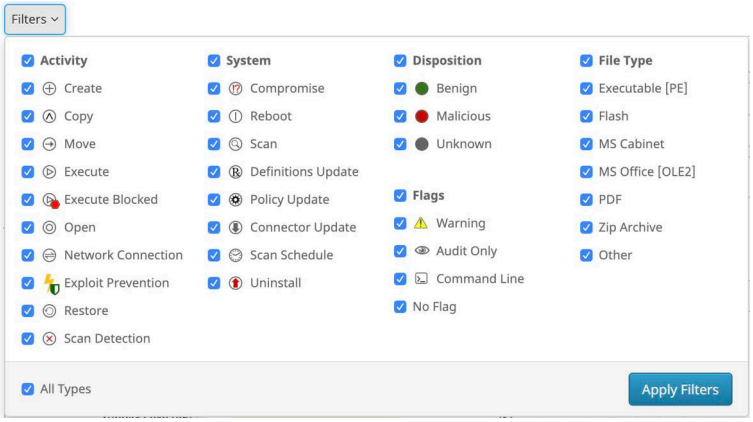
For indication of compromise descriptions, see Indicators.

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 five event filter categories in Device Trajectory: Activity, System, Disposition, Flags, and File Type. You must select at least one item from each category to view results.



Activity describes events that the 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.

System events can include compromises, reboots, policy or definition updates, scans, and uninstalls.

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.

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 **Files and Network Conviction Modes** policy items under Modes and Engines were 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.

You can search Device Trajectory events by the following terms:

- Detection name
- SHA-256
- Filename
- File path
- URL
- Remote IP addresses
- User name
- iOS Bundle ID

To perform a search, enter or paste the search term in the search field and press Enter.

To copy a SHA-256 to the clipboard:

- Right-click a file or process on the vertical axis of the Device Trajectory and select Copy SHA-256 from the menu.
- In the Event Details panel, click the pivot menu button next to the SHA-256 and select Copy to Clipboard or click the button.

Mobile App Trajectory

Mobile App Trajectory shows activity for a specific app from all devices running Secure Endpoint iOS Clarity with that app installed. This can be useful in locating unwanted or suspicious activity. Launch the Mobile App Trajectory by clicking the **App Trajectory** link on the Dashboard iOS Clarity tab or by clicking a bundle ID and selecting Mobile App Trajectory from the context menu.

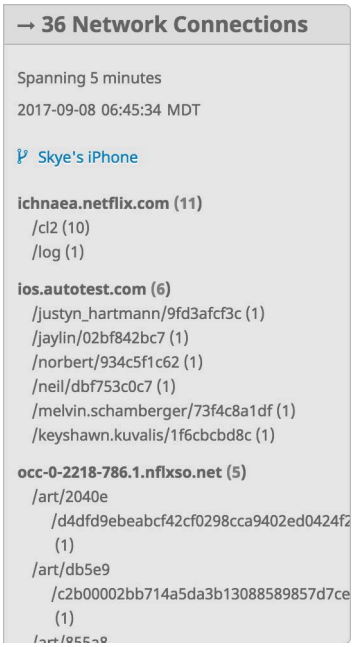
The top of the page shows a summary of all information that can be gathered about the app including the version and publisher.

You can use the date slide to choose three days to view. The blue dots on the days indicate the amount of activity observed from that app.

The **Endpoints using this App** section shows a list of devices with network activity from that app for the 3 day period selected in the slider. The vertical axis shows the list of devices with the app installed and the horizontal axis represents the date and time. The length of each arrow indicates the amount of activity the app was observed generating. Click a device name to view its **Device Trajectory** for a full view of all app activity on that device.

You can also click on a day to zoom and show three 8 hour columns. You can continue to zoom to 2 second intervals.

Click on an arrow to show details about the activity, including the number of connections and duration, specific times, and details of each network connection.



Network Destinations provides a list of all domains accessed by the device organized by top-level domain (TLD). The list can be sorted alphabetically or by total number of connections. You can expand entries to view additional details and specific URLs, ports, and connections.

Chapter 19
File Repository

The File Repository allows you to download files you have requested from your 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. Files that were automatically sent for analysis from Automatic Analysis and Behavioral Protection will also be available in the repository.

IMPORTANT! You must have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication 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 Secure Endpoint Windows connector, version 1.0.2.6 or later of the Secure Endpoint Mac connector, and version 1.0.2.261 or later of the Secure Endpoint 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 Secure Endpoint 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.

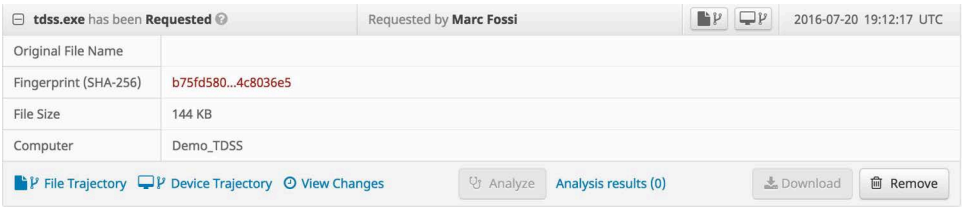
A dialog will appear allowing you to select which connector to download the file from. If the file was observed by more than one connector, you can use the drop-down list to select a specific computer out of up to ten computers that saw the file recently. The default selection is the connector that observed 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 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 20
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.

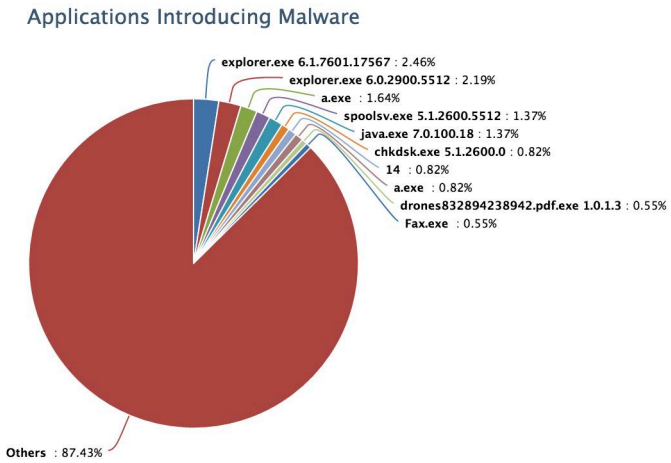
Select Dates

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.

Threat Root Cause 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.

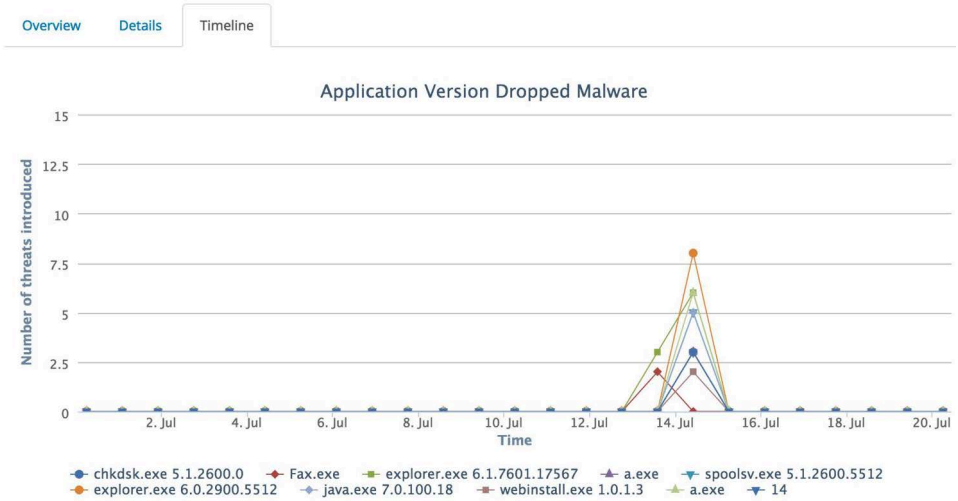
Program	Threat Name	Version	Threats Introduced	Computers Affected	Event Type
explorer.exe		6.1.7601.17567	9	3	6 created 3 executed
explorer.exe		6.0.2900.5512	8	4	4 executed 4 moved
a.exe			6	1	2 created 2 executed 2 moved
spoolsv.exe		5.1.2600.5512	5	1	3 created 2 executed
java.exe		7.0.100.18	5	1	3 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 21
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. Secure Endpoint will request the file from the connectorthat 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 Secure Malware Analytics API key on the Organization Settings page and they can be up to 20MB each in size.

Chapter 22
Vulnerable Software

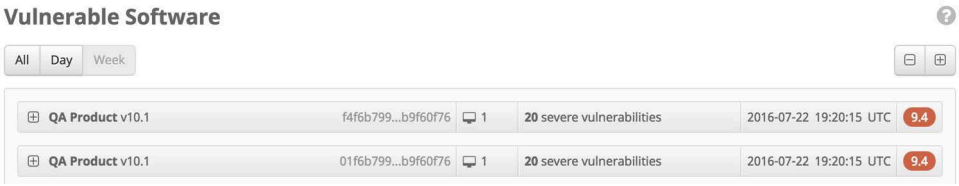
Whenever an executable file is moved, copied, or executed the Secure Endpoint connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) 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 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

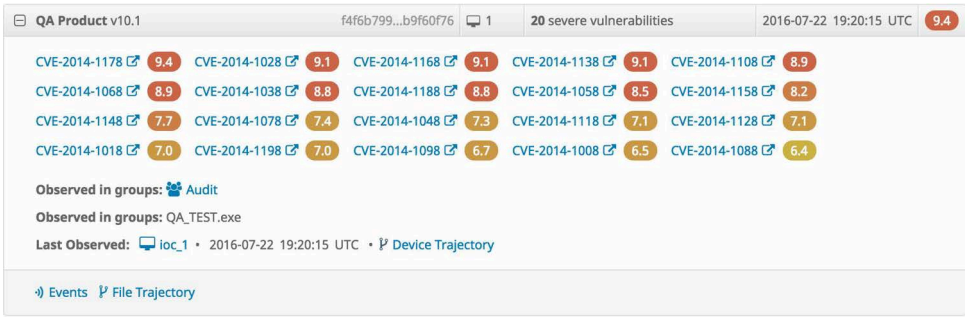
The Common Vulnerabilities and Exposures (CVE) database records known vulnerabilities in various applications. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the console can be clicked to get more details on the vulnerability.

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.

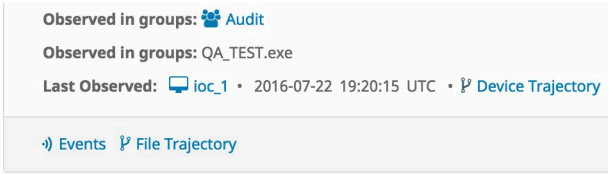


Additional Information on Vulnerable Software

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 computer 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 23
Reports

Reports allow you to view aggregate data generated in your organization over a one-week, one-month, or three-month (quarterly) period. They can be accessed from **Analysis > Reports** on the main menu. Click the title to view any of the reports, and you can sort the list by clicking the heading of any of the columns.

Create a Custom Report

Weekly reports cover a one-week period beginning every Sunday at midnight until midnight the following Sunday (UTC). Monthly reports cover a period beginning on the first day of the month at midnight until midnight on the last day of the month. Quarterly reports cover a period beginning on the first day of the month at midnight and ending three months later on the last day of the month. System-defined reports are created automatically but you can configure your own custom reports.

Configure Custom Reports

You can create, edit and delete reports and choose whether to receive them via email from the report configuration page. Click the Configure Custom Reports button on the Reports page to access this page. You can view changes to a single report configuration by clicking the View Changes button  in one of the rows, or all the report configurations by clicking View All Changes.

Create Reports

You can create custom reports to view information about selected groups of computers. Click the New Custom Report button on the Report Configuration page to display the New Custom Report dialog. Select the report type (weekly, monthly, or quarterly), enter the title for the report and select the groups you want to include in the

report from the drop-down menu. Fill the Email checkbox if you want to receive the reports via email, and click Save and Schedule.

Edit Reports

Click the Edit button in the row of the report you want to edit. You can modify the title and selected groups in the dialog box and click Save and Schedule when done.

IMPORTANT! You cannot edit system-defined reports.

Delete Reports

Click the Delete button in the row of the report you want to delete and confirm deletion in the dialog box by clicking Delete.

IMPORTANT! You cannot delete system-defined reports. However, you can clear the **Email** checkbox for it if you do not want to receive it.

Report Sections

Elements in the reports (E.g. SHA-256, computers, threats) link to the appropriate sections of the Secure Endpoint console, so you can drill down further into the data.

Some sections contain boxes highlighting important metrics. The little numbers and arrows inside these boxes display week-to-week trends and when applicable, are green or red to provide “good” or “bad” context, respectively.

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 organization compared to the previous week. To be considered active, a connector must have checked in at least once in the reporting period. The number of new installs and uninstalls are also shown.

Connector Status

This shows the number of files and IPs that were scanned during the reporting period, along with the number of active connectors as of the last day of the reporting period. To be considered active, a connector must have checked in with the Secure Endpoint servers at least once in the reporting period. This section also displays information about your current license compliance for your organization as of the last day of the reporting period.

Compromises

New Compromises are a result of threat detections or malware execution on an endpoint. The number of compromises still open from the previous reporting period are shown along with the number of compromises resolved in the current reporting period. Compromises in the graphs are color-coded by severity. The tables show the top 5 Significant Compromise Observables from the reporting period, and Compromise Event Types with their respective severity from the reporting period.

File Detections

Shows the number of computers in your organization that observed the highest number of malicious file detections along with the most frequently seen detections. The daily malware detections can show any trends about which days of the week computers see the most detections. Computers with high numbers of file detections may be indicative of a dropper infection.

Network Detections

Shows the number of device flow correlation detections and agentless global threat alerts in your environment as well as the number of computers in your organization that observed malicious network detections. The daily network detections can show any trends about which days of the week computers see the most network detections. High numbers of network detections may be indicative of a bot infection.

Device flow correlation metrics only apply to connectors with device flow correlation enabled in their policies, and agentless global threat alerts require a global threat alerts device to be installed.

Blocked Applications

Shows how many applications that your connectors blocked from executing. connectors only block applications that you have added to your blocked application lists (see Application Control - Blocked Applications).

Low Prevalence Executables

Shows the number of Low Prevalence Executables sent for analysis, the number of threats detected in those submissions, and the actions taken. Submission Limit is the percentage of your total submissions available to be sent for analysis during the reporting period. Unique Detections are the number of Low Prevalence Executables that were determined to be malicious.

Threat Root Cause

Shows the applications that have been observed introducing the most malware into your environment within the reporting period. With this information, you can quickly identify applications that are frequently utilized by malware to remain resident on — or gain access to — computers in your environment. The (other) entry is an aggregate of all other applications that have introduced malware into your environment.

Vulnerabilities

Shows the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint 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. The Top Vulnerable Applications table displays the top vulnerable applications in order of severity, the version number, the number of executions, the number of CVEs, and their severity. The Top Vulnerable Computers table displays the top vulnerable computers and the number of vulnerable applications on the computers.

Successful Quarantines

Shows the number of files that were quarantined by your connectors each day. Note that not all detections result in a file being quarantined by the connector. In some cases your antivirus software may have already quarantined the file or the file was deleted before it could be quarantined.

Retrospective Detections

Shows the number of files that were seen by your connectors but later 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

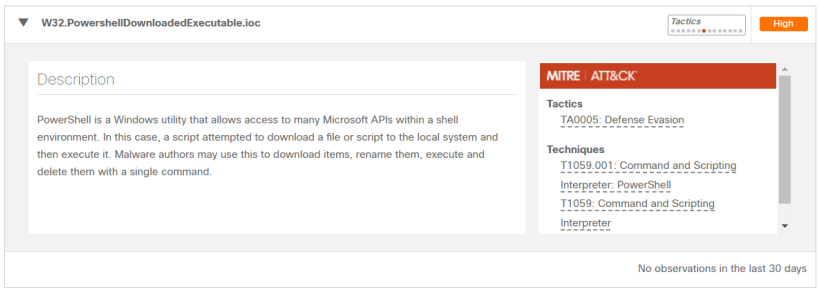
Shows the number of times Trajectory Indications of Compromise were triggered for the week.

CHAPTER 24
INDICATORS

Secure Endpoint determines Cloud Indications of Compromise (IOCs) based on multiple events or sequences of events observed on an endpoint within a certain time period. The purpose of a Cloud IOC is to act as a notification of suspicious or malicious activity on an endpoint. A Cloud IOC trigger on a host needs to be investigated further to determine the exact nature and source of suspicious activity outlined in the IOC description. A single Cloud IOC will only be reported once every four hours per endpoint.

The Indicators page lets you search for Cloud IOCs and Behavioral Protection signatures. You can access the page from **Analysis > Indicators** on the main menu. Each indicator includes a brief description along with information about the tactics and techniques employed based on the Mitre ATT&CK knowledge base. Tactics represent the objective of an attack, such as executing malware or exfiltrating confidential information. Techniques are the methods attackers use to achieve the objectives or what they gain. For more information, see Getting Started with ATT&CK.

You can search for specific indicators by name, or filter the list based on tactics, techniques, and severity. The number of compromises in your organization that are associated with an indicator are also shown and you can filter the list to only display these.



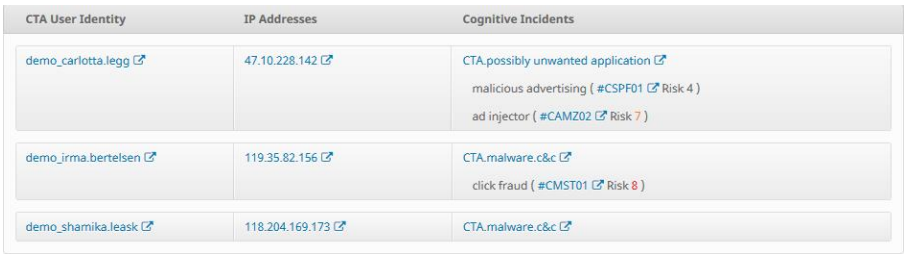
Click on an indicator to expand the description and display the full list of tactics and techniques. Click on any tactic or technique for a detailed description.

Click a compromise badge to see a filtered view of the Inbox Tab of all endpoints that have observed the indicator. Click the Dashboard, Events, or Inbox links to see a filtered view of those pages showing only the computers that observed the indicator.

Chapter 25
Agentless Global Threat Alerts

Agentless incidents are events recorded by global threat alerts for your organization. This records incidents that occur on computers that don't have a Secure Endpoint connector installed. You must have Global Threat Alerts Integration enabled on the Organization Settings page and at least one enabled device like a Cisco Secure Web Appliance (formerly Web Security Appliance) configured to send logs to global threat alerts for events to populate this page.

Each row has a username (if it can be determined), IP address, and list of global threat alerts that were detected by your 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 alert 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 global threat alerts 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 a connector on any computers that appear in the Agentless Global Threat Alerts 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 26
Accounts

Items under the Accounts menu allow you to manage your Secure Endpoint 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 filter the user list by various fields and settings. **Last Login** allows you to view users who have logged in during various time frames or never. **User** lets you search by username or email address. The Two-Factor Authentication, Remote File Fetch, and Command Line filters allow you to filter by whether users have those features enabled or not on their accounts.

You can sort the list of users 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.

To view and edit details of an account, click the name of a user to access the user account page. If you select your own account you also have the option to reset your password.

IMPORTANT! You can send an email notification to a user to enable Two-Factor Authentication from the user account page.

Click on New User to create a new Secure Endpoint console user account. A valid email address is required for the new user to receive an account activation email. The email will provide instructions to create and log in with their required Cisco Security Cloud sign-on account. 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 Secure Endpoint 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 My Account 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

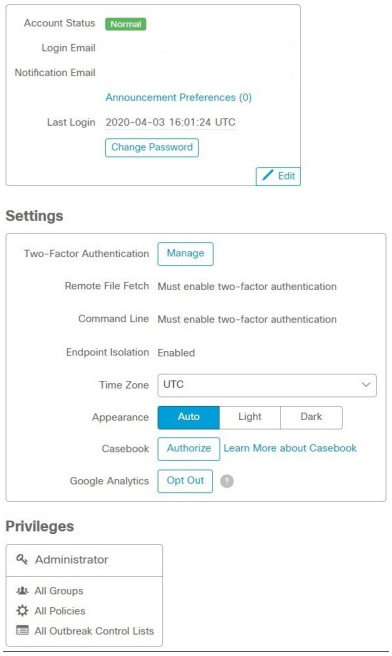
To change the time zone displayed by the Secure Endpoint console for your user account:

1. Click My Account or go to the Users page and click on your name or email address.
2. Select your preferred time zone settings from the Time Zone drop-down menu.

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.

My Account

Users can access their account settings on this page by clicking **My Account**.



Password reset, Two-Factor Authentication, Time Zone Settings, Appearance, and Authorize Casebook are on this page. Users can choose the types of announcements that they receive by email by clicking the **Announcement Preferences** link.

Appearance settings allow you to manually select Light or Dark themes for the Console, or select Auto to use the theme selected through the operating system settings on versions of Windows, macOS, and iOS that support it.

Secure Endpoint collects usage data with **Google Analytics** to improve accuracy, improve the product and help troubleshoot issues. Users can choose to opt out their own account from Google Analytics by clicking the Opt Out button.

IMPORTANT! The Opt Out button affects only the user, not the organization. Use the setting under Features on the Organization Settings page to opt the entire organization out of Google Analytics.

You can choose to opt in to UX Research. This invites you to participate in studies for early Secure Endpoint designs and features.

Access Control

There are two types of users in Secure Endpoint, 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 Secure Endpoint 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
- Create Device Control configurations
- Change Organization Settings
- Enable Demo Data
- View Command Line 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. There are also options to allow the user to:

- Fetch files and diagnostics from computers in the selected groups.
- View command line data from the selected groups.
- Set Endpoint Isolation status for the selected groups.

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.

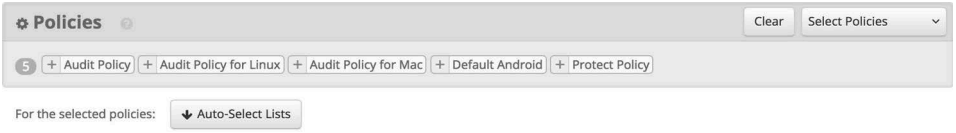
The user will be able to view these groups on the Groups page but not be able to make any changes or create new groups. The user will also be able to view information from connectors in these groups, such as:

- Dashboard Overview Tab, Events Tab, iOS Clarity 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 or view Command Line data in Device Trajectory and Events Tab. The user will need to have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication enabled before they can view the repository, request files, or see command line data on the trajectory page. You can uncheck either of these boxes at any time to remove these permissions.

IMPORTANT! Unprivileged users can only request and view files and command line data 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 policy objects associated with the groups you selected. The **Clear** button will remove all policies the user has been given access to.



Next, you can select Policy Objects the same way. Policy objects consist of custom detection lists, application control lists, IP block and allow lists, exclusions, and device control configurations. Either select individual lists or click the auto-select button to populate the 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.

IMPORTANT! IP block and allow lists can be added to policies by users who haven't been granted permissions to those lists. The users are still unable to view or edit those lists.

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-factor authentication.

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-Factor Authentication

Two-factor authentication provides an additional layer of security against unauthorized attempts to access your Secure Endpoint 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.

IMPORTANT! Because multi-factor authentication is included in Security Cloud sign-on, the two-factor authentication option in the console is redundant and is disabled for all accounts that use Security Cloud sign-on. All the features that require two-factor authentication are enabled for Security Cloud sign-on users.

You can enable two-factor authentication for your account by clicking on **Enable** or **Manage** next to the Two-Factor Authentication entry on your account in the Users page.

You will then be guided through the steps to enable two-factor authentication 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-factor authentication on your account, you will now see a button to view two-factor authentication Details.

If you need to disable two-factor authentication or generate new backup codes, click this link to return to the two-factor authentication setup page.

The next time you log in to the Secure Endpoint 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-factor authentication 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-factor authentication, 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 Secure Endpoint 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. You can also select to allow the API credential access to Command Line capture data. The account used to make API requests for command line data must have administrator privileges and single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication enabled.

IMPORTANT! An API credential with read and write scope can make changes to your Secure Endpoint configuration that may cause significant problems with your endpoints. Some of the input protections built into the Secure Endpoint 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.

When you enable Cisco XDR or SecureX Integration, there will be an auto-generated API credential created. These credentials will have read/write permissions and be named [AUTO-GENERATED] SecureX Module API Client. These credentials are also used to create an install token for Cisco Secure Client.

Organization Settings

The Organization Settings screen allows you to specify global defaults for your Secure Endpoint deployment.

The Organization Name entry appears on all reports that are generated from your Secure Endpoint deployment. Click Edit to change the Organization name and add up to three Preferred Contact email addresses. The Preferred Contacts may be used for support escalations, Threat Hunting, or Talos Intelligence Group to reach out to.

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 each connector type for any new groups that are created unless one is specified, or they inherit one through their parent. The Default connector Version allows the administrator to specify which version of each connector will be installed during new deployments.

Click Update to save your changes for this section.

Features

The Features section of the Organization Settings page allows you to enable or disable certain features and define interaction with Cisco Secure Malware Analytics.

Enable Request and store files from endpoints to use the File Repository. This setting applies to all users in your organization. You will need to have single sign-on (such as Security Cloud sign-on) or Two-Factor Authentication enabled on your account and provide your verification code.

3rd Party API Access allows you to use the application programming interfaces to access your Secure Endpoint data and events without logging into the console. You can generate the API key from the API Credentials page. For more information, see the Secure Endpoint API documentation.

Mobile Device Manager shows which MDM Integration you currently have set up to use and deploy the Secure Endpoint iOS Connector with Clarity on iOS devices. Click MDM Integration to select your MDM or change your Meraki SM API key.

You can click to configure **Single Sign-On** if your organization has not migrated to Security Cloud sign-on. This will allow your users to log in to the Secure Endpoint Console using their single sign-on credentials once configured. You cannot use Two-Factor Authentication with single sign-on enabled, but all features requiring two-factor authentication will be enabled.

You can enter your Secure Malware Analytics API key, if you have a separate Cisco Secure Malware Analytics account. This allows you to see analysis results from your Secure Malware Analytics account in File Analysis. When you enter a Secure Malware Analytics 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 Secure Malware Analytics 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 Global Threat Alerts (formerly Cognitive Threat Analytics) account linked to your Secure Endpoint organization. This will also configure single sign-on between the two systems so that you can use your Secure Endpoint credentials to log in to global threat alerts. You will then be able to configure web log uploads from Secure Endpoint to global threat alerts for processing. To allow unprivileged users to view global threat alerts events, contact support.

IMPORTANT! If you are already a global threat alerts customer, contact support to link your existing account to your Secure Endpoint organization. Otherwise, using the Configure button will create a separate empty global threat alerts account.

The **AV Definitions Threshold** setting lets you configure the number of days (between 1 and 7) stale that connector AV definitions can be before they appear as outdated on the Computer Management page.

Secure Endpoint collects usage data with Google Analytics to improve accuracy, improve the product and help troubleshoot issues. You can choose to opt out the organization from Google Analytics by clicking the Opt Out button.

The Inactive Computer Threshold allows you to specify how many days a connector can go without checking in to the Cisco cloud before it is removed from the Computer Management page list. The default setting is 90 days. Inactive computers will only be removed from the list and any events they generated will remain in your Secure Endpoint organization. The computer will reappear in the list if the connector checks in again.

IMPORTANT! Licenses are not reclaimed when the connector is removed from the computers page list.

Cisco XDR or SecureX Integration

Cisco XDR or SecureX connects Cisco's integrated security portfolio and your infrastructure for a consistent experience. It delivers unified visibility with shared context and meaningful metrics, built-in integrations with out-of-box interoperability, and strengthens your security by accelerating threat investigations and remediation across your security ecosystem.

Cisco XDR or SecureX integration allows you to integrate your Secure Endpoint organization with your Cisco XDR or SecureX account. When it is enabled it will share some of your Secure Endpoint data with Cisco XDR or SecureX.

The Secure Endpoint module in Cisco XDR or SecureX can display:

- Compromises
- Compromises over time
- Quarantines
- Quarantines over time
- Vulnerabilities
- Computers
- Computers not seen in over 7 days
- Computers with out of date definitions
- Computers with out of date connector versions
- MITRE ATT&CK tactics and techniques observed

Incident promotion is enabled automatically when you enable Cisco XDR or SecureX integration. This allows incidents to be promoted to Cisco XDR or SecureX threat response incident manager to be streamlined. Compromises automatically promoted to Cisco XDR or SecureX are automatically investigated to be enriched with additional threat context available in Cisco XDR or SecureX threat response. You can disable incident promotion and keep Cisco XDR or SecureX integration enabled. See Cisco XDR incidents or SecureX threat response for more information.

All low, medium, high, and critical severity incidents will be promoted to Cisco XDR or SecureX by default. You can adjust the severity threshold if you feel that too many incidents are promoted and you only want to see more severe incidents. We

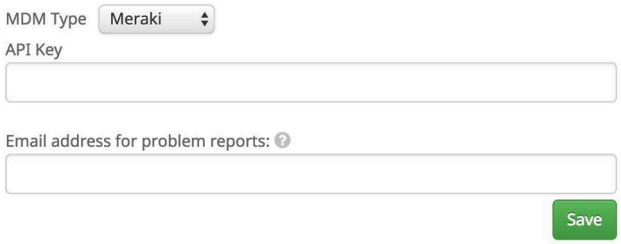
recommend that you start with the low severity setting and gradually step up until you find the severity threshold that works best for you.

IMPORTANT! If you previously integrated your Secure Endpoint organization with SecureX, you should delete the old Secure Endpoint module in SecureX and only use the new module. New modules allow for two-way data exchange, while the old modules were only a single direction.

Enabling Cisco XDR or SecureX integration will also create API Credentials in your organization. These credentials will have read/write permissions and be named [AUTO-GENERATED] SecureX Module API Client. These credentials are also used to create an install token for Cisco Secure Client.

MDM Integration

Before you can deploy the Secure Endpoint iOS Connector on iOS devices you must connect your Mobile Device Manager to the Secure Endpoint console on the MDM Integration page. You can also provide an email address that will be displayed on Clarity endpoints for users to contact if they experience any problems.



Meraki

You will need to provide the API key from your Meraki SM to deploy the Clarity on your iOS devices. For information on configuring your Meraki SM, see the Meraki SM Clarity configuration page.

On the Meraki Dashboard:

1. Go to **My Profile**.
2. Under **API Access** select your API key and copy it.

On the Secure Endpoint Console:

1. Go to the **Dashboard** page and select the **iOS Clarity** tab.
2. Click the **MDM integration** link.
3. Paste your Meraki API key into the **API Key** field. You can change your API key at any time from the Organization Settings page.
4. Enter an email address that will be displayed in the Clarity app for users to contact if they experience any problems.
5. Click **Save**.

If you need to make changes or add more Groups to your Meraki SM you can do this from the Deploy Clarity page by navigating to **Management > Deploy Clarity for iOS**.

Workspace ONE

You will first have to add Clarity to your Workspace ONE MDM. From the Workspace ONE Dashboard:

1. Navigate to **Apps & Books > Public Tab**.
2. You should see the Clarity app listed. If not, click **Add Application**.
   - Select Apple iOS for platform and search for "Clarity".
   - Select the application from the search results then click **Save & Assign**.
3. Click **Select Assignment Groups > Create Assignment Group** to create a new Smart Group.
   - Assign a **Name** to the Smart Group.
   - Set **Ownership** to **Shared** and **Corporate**.
   - Set the **Platform and Operating System** to **Apple iOS**, **Greater Than**, and **iOS 11.2.0**.
   - Click **Save**.
4. The first time you add the Clarity you may see the Add Assignment dialog.
   - Set **App Delivery Method** to **Auto**.
   - Set **Managed Access** to **Enabled**.
   - Set **Make App MDM Managed if User Installed** to **Enabled**.
   - Click **Add**.
5. Click **Save & Publish** then click **Publish**.
6. Select the Clarity app under **Apps & Books**. On the Assignment tab make sure your Smart Group is listed.

From the Secure Endpoint Console:

1. Navigate to **Accounts > Organization Settings**.
2. Under Features click **MDM Integration**.
3. Select Workspace ONE from the **MDM Type** pull-down menu.
4. Enter an email address that will be displayed in the Clarity app for users to contact if they experience any problems.
5. Click **Save**.

MobileIron

You will first have to add the Clarity to your MobileIron MDM. From the MobileIron Dashboard:

1. Navigate to **Devices & Users > Labels**.
2. Click **Add Label**.
   - Assign a **Name and Description** to the new Label.
   - Add a **Criteria** with the settings **Platform Name**, **Starts with**, and **iOS 11.2**.
   - Add another **Criteria** with the settings **Supervised**, **Equals**, and **true**.
   - Click **Save**.
3. Navigate to **Apps > App Catalog** and click **Add**.
4. Click **iTunes** and search for the Clarity.

5. Select Clarity from the search results and click **Next**.
6. Most of the fields on the next page are already populated. Add a **Description** and **Category** then click **Next**.
7. Select **Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in** then click **Next**.
8. Navigate to **Apps > App Catalog**.
    - Select **Actions > Apply to Labels**.
    - Select the label you created in Step 2.
    - Click **Apply**.

From the Secure Endpoint Console:

1. Navigate to **Accounts > Organization Settings**.
2. Under Features click **MDM Integration**.
3. Select MobileIron from the **MDM Type** pull-down menu.
4. Enter an email address that will be displayed in the Clarity app for users to contact if they experience any problems.
5. Click **Save**.

Other MDMs

From the Secure Endpoint Console.

1. Go to **Accounts > Organization Settings**.
2. Under Features click **MDM Integration**.
3. Select Generic from the **MDM Type** pull-down menu.
4. Enter an email address that will be displayed in the Clarity app for users to contact if they experience any problems.
5. Enter the MDM's configuration variables for Serial Number and MAC Address, respectively.
6. Click **Save**.

IMPORTANT! For Clarity to work properly, both the Serial Number and MAC Address configuration variables must be entered.

Remove MDM Integration

To remove MDM integration, navigate to the Organization Settings page, click the Edit button, then click the Delete button beside MDM integration.

Single Sign-On

Single sign-on (SSO) streamlines the user login process while enhancing security. SSO involves three parts: the user, third-party identity provider (IdP), and your Secure Endpoint account. Once SSO is enabled, authentication takes the following steps:

1. The user connects to the Secure Endpoint SSO login page and attempts to authenticate by entering their username.
2. If the username is valid, the user's authentication request is redirected to the third-party identity provider.
3. The third-party identity provider validates the user.
4. On successful authentication, the user gains access to the their account.

Secure Endpoint single sign-on supports SAML 2.0. You can configure Secure Endpoint to use Cisco Secure Sign-On, or you can use a custom third-party identity provider. This document assumes your identity provider is set up with your users. You can learn more about Cisco Secure Sign-On at https://cisco.com/go/securesignon.

Caveats

Keep the following caveats in mind when enabling single sign-on for your organization:

- All users must have an account with an email address that has a corresponding email address at the identity provider. If you have any users who do not have a matching email address at the identity provider, those users will no longer be able to log in. Contact support to have single sign-on disabled for those users.
- Using Cisco Secure Sign-On as your SAML provider requires all accounts in your organization to have existing Cisco Secure Sign-On accounts. You can create Cisco Secure Sign-On accounts at https://sign-on.security.cisco.com. Users will receive an email and must activate their accounts within 7 days. Users without an account will not be able to sign in.
- All user passwords will be reset to prevent users from logging in using the standard username and password mechanism. Admin users will be able to create a one-time password.
- Two-factor authentication will be disabled for each user. You will need to re-enable two-factor authentication if you disable single sign-on.
- Contact support if you need a user with Secure Sign-On disabled.

Enable Single Sign-On Using Cisco Security Cloud Sign-On

To enable Cisco Security Cloud Sign-On for your organization:

1. Log in to your Secure Endpoint administrator account.
2. Go to **Accounts > Organization Settings**.
3. Click the **Configure Single Sign-On** link.
4. Select **Cisco Security Cloud Sign-On**. This takes you to the SAML Configuration page.

5. Go to https://sign-on.security.cisco.com and click **Sign up** to create a Cisco Security Cloud Sign-On account. For more information about creating this account, see Cisco Security Cloud Sign-On Quick Start Guide.

   IMPORTANT! Using Cisco Security Cloud Sign-On as your SAML provider requires all accounts in your organization to have existing Cisco Security Cloud Sign-On accounts. You can create Cisco Security Cloud Sign-On accounts at https://sign-on.security.cisco.com. Users without an account will not be able to sign in.

6. Once your account is created, return to the SAML Configuration page, and click **Verify Configuration**.
7. Sign in with the credentials provided when you created the Cisco Security Cloud Sign-On account. You are prompted to log in with Duo Security as a second authentication factor.
8. Once you have verified your configuration, note the caveats listed on the SAML Configuration page then click **Enable Cisco Security Cloud Sign-On** to complete the setup.
9. An email is sent to each user with instructions on how to log in. Instead of entering their username and password, users must now log in by clicking **Use Single Sign-On** on the log in page, entering their email address, then clicking **Log In**. If the user has not already authenticated to the identity provider they are redirected to do so.

Enable Single Sign-On Using Custom Single Sign-On

To enable single sign-on for your organization using your existing third-party identity provider:

1. Log in to your Secure Endpoint administrator account.
2. Go to **Accounts > Organization Settings**.
3. Click the **Configure Single Sign-On** link.
4. Select **Custom Single Sign-On**. This takes you to the SAML Configuration page.
5. Enter the information provided under **Service Provider Settings** into the appropriate setup page on your identity provider. The items may have different names on your identity provider's system. For example:
   - **Assertion Consumer Service URL** may be called **SAML Assertion Consumer Service (ACS)** or **Single Sign-on URL**.
   - **Entity ID** may be called **SP Entity ID** or **Audience URI**.
6. Enter any additional information your identity provider requires, noting the following:
   - For Active Directory set **Outgoing Claim Type** to **Email Address**.
   - For Okta set **Name ID format** to **EmailAddress** and **Application username** to **Email**.
7. Download the SAML metadata file from your third-party identity provider or copy the SAML metadata URL.

8. Under **Identity Provider Settings**, upload the SAML metadata file or paste the SAML metadata URL.
9. Click **Save SAML Configuration**.
10. Click **Test** to test your configuration. You are prompted to log in to your identity provider. If the test is successful, move on to the next step.
11. Click **Enable SAML Authentication** to complete the setup.

An email is sent to each of your users with instructions on how to log in. Users must log in by clicking **Use Single Sign-On** on the log in page and entering their email address.

Disable Single Sign-On

To disable single sign-on for your organization:

1. Log into your Secure Endpoint administrator account.
2. Go to **Accounts > Organization Settings**.
3. Click the **Configure Single Sign-On** link.
4. Click **Disable SAML Authentication** to disable single sign-on.

A password reset email is sent to all single sign-on users in your organization who had single sign-on enabled. Users must reset their password before they can log in to the Secure Endpoint console.

IMPORTANT! If you are the administrator who is disabling single sign-on, you can reset your password immediately. You do not need to wait for the password reset email.

License Information

Your current license information is displayed on this page. The top of the page shows whether your organization is compliant, the number of seats in use and how many you have available. Your licenses and their start and end dates are also shown.

Audit Log

The audit log allows the Secure Endpoint 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. Audit log entries are stored for three years.

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 Secure Endpoint 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 Secure Endpoint console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, Detections, and Events behave when malware is detected. You can also test the Endpoint Isolation feature by starting and stopping a simulated isolation session.

IMPORTANT! The group policy for the Demo Data computers must have Endpoint Isolation enabled to simulate an isolation session. Endpoint Isolation is available for Windows connector versions 7.0.5 and later and Mac connector versions 1.2.1 and later.

Demo Data can coexist with live data from your Secure Endpoint 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.

Applications

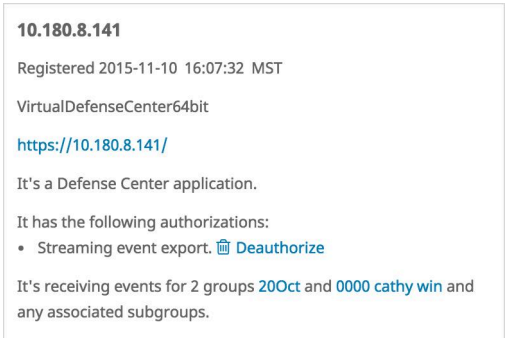
The Applications menu shows which applications external to Secure Endpoint you have authorized to access your organization's data. For example, you can display Secure Endpoint data in your Cisco Secure Firewall Management Center dashboard.

For more information on Secure Firewall integration with Secure Endpoint, see your Secure Firewall 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 Secure Endpoint entirely.

Application Settings

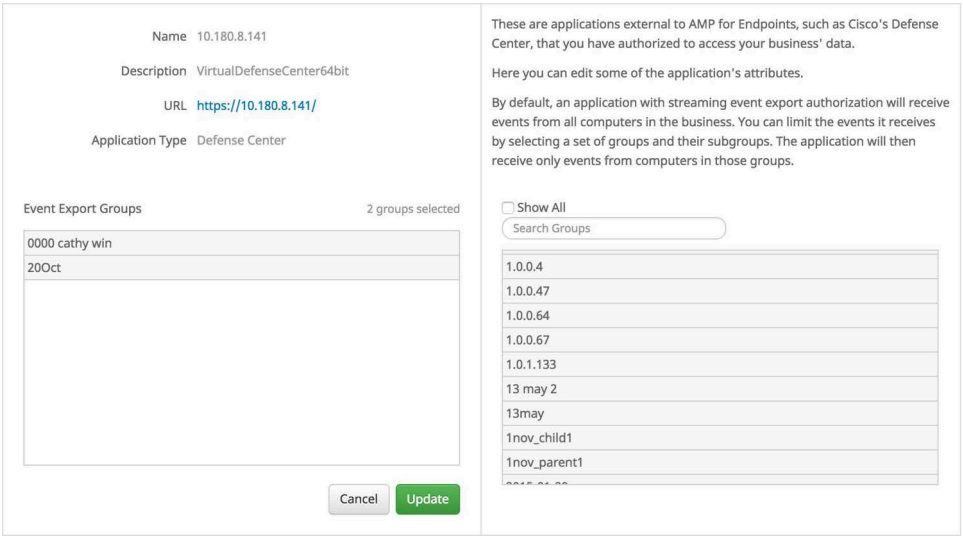
When you select the name of an application from your list you will see the current settings for that application.



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 Secure Endpoint 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 Secure Endpoint entirely, you must deregister it from the main Applications screen.

Chapter 27
AV Definition Summary

This page displays the latest antivirus definition versions available so that you can track when definition updates became available.

Each of the boxes at the top displays the latest definition versions available for each operating system. Each of the tabs contains a list of the selected operating system's AV definition versions. You can click on the boxes or the tabs to select the operating system. For Secure Endpoint Linux connectors you can view endpoints with the full ClamAV definition set or those with the Linux-only definition subset.

Chapter 28
SecureX

Cisco SecureX connects Cisco's integrated security portfolio and your infrastructure for a consistent experience. It delivers unified visibility with shared context and meaningful metrics, built-in integrations with out-of-box interoperability, and strengthens your security by accelerating threat investigations and remediation across your security ecosystem. The SecureX ribbon in the Secure Endpoint console carries the most relevant security context from your products to enhance investigations and pivots.

Activate SecureX

You must link your Secure Endpoint account to SecureX using your Cisco Security Cloud Account.

1. Click the SecureX ribbon at the bottom of your Secure Endpoint console.
2. Click **Get SecureX**.
3. Click **Log in with Cisco Security Cloud Sign-On**.
4. Click **Authorize Secure Endpoint**. This allows your data to be shared between Secure Endpoint and SecureX.

The Secure Endpoint module in SecureX can display:

- Compromises
- Compromises by endpoint
- Compromises over time
- Top Compromise observables
- Endpoint malware threats
- Quarantines
- Quarantines over time
- Vulnerabilities

- Computers
- Computers not seen in over 7 days
- Computers with out of date definitions
- Computers with out of date connector versions
- MITRE ATT&CK tactics and techniques observed
- SecureX Threat Hunt (Premier package only)

SecureX Ribbon

You can use the SecureX ribbon to launch your other Cisco security applications, and work with investigations and incidents using Casebook, Threat Response, and Orbital. You can also use the **Find observables on page** button to find any data points on the current page of your Secure Endpoint console to add to a Casebook case or investigate further in Threat Response.

For more details on configuring and using SecureX see the documentation on the SecureX dashboard. Open the ribbon and click Launch next to SecureX, then click the help icon at the top right of the page.

Casebook

Casebook is a tool for saving, sharing and enriching analysis by adding file hashes, IPs, domains, log entries, etc. into an ongoing investigation and submitting entire cases to Cisco Threat Response. Investigators can add notes, descriptions and sync an active casebook across tabs as well as export cases for use in other tools and systems.

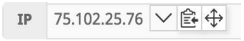
You can access Casebook from the SecureX ribbon to create cases and to add and look up observables such as IPs, domains, and SHA-256s. For more information, see Cisco Threat Response Help.

Pivot Menu

When SecureX is enabled, you can click the pivot menu button ⌄ next to observables on any page to access actions from Cisco Advanced Threat Solutions, like Umbrella, Talos, Secure Malware Analytics, Cisco Threat Response, etc. The pivot menu replaces the SHA-256 File Info Context Menu.

IMPORTANT! The features displayed in the pivot menu depend on the kind of observable you are investigating.

When hovering over the pivot menu, you will see two buttons that you can click to copy the observable to the clipboard, and to click and drag it into Casebook, respectively.



Chapter 29
Secure Endpoint Update Server

The Secure Endpoint Update Server is designed to reduce the high volume of network traffic consumed by the Secure Endpoint Windows connector while fetching TETRA definition updates from Cisco servers. The utility aims to reduce the update bandwidth consumption by acting either as a caching HTTP proxy server, or by periodically fetching updates to a location that can be served by an on-premises HTTP server that you must set up and configure. You must enable your Local Secure Endpoint Update Server under the TETRA section of your Windows policies. It may take an hour or longer for the Secure Endpoint Update Server to download initial content from the malware analytics cloud.

IMPORTANT! Only Secure Endpoint Windows connector 5.1.13 and later can use a local Secure Endpoint Update Server.

Requirements

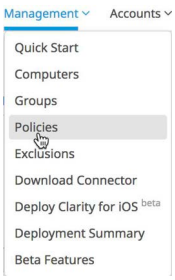
The Secure Endpoint Update Server is supported on Window Server 2012 and higher and CentOS release 6.9 (Final) x86_64. Supported Web servers are Apache, Nginx, and IIS.

Hardware Requirements

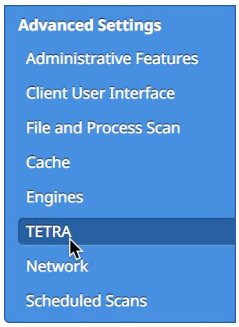
- 8 core CPU.
- 16 GB RAM.
- 100 GB free disk space.

Download the Secure Endpoint Update Server

1. Navigate to Management > Policies.



2. Select a Windows policy and click Edit.
3. Go to Advanced Settings > TETRA in the policy.



4. Click the Secure Endpoint Update Server Configuration link.
5. Click the Download button for your server operating system. You will need to transfer this archive to your server and extract the files.
6. Select the Interval that your server will check the malware analytics cloud for updates and click the Download button. You will need to transfer the config.xml file to the same location on your server as the archive from step 5.
7. Once you have configured the Secure Endpoint Update Server you will have to return to the TETRA section of each policy you want to use it on to enable and configure it.

Fetch-Only Mode

In this mode, the Secure Endpoint Update Server is used to fetch TETRA definition updates to a user-specified location. You must set up an HTTP server such as Apache, Nginx, or IIS to serve the downloaded content. The recommended configuration is to set this up as a Scheduled Task on Windows or a Cron job under Linux.

Fetch-Only Single Update Mode

This mode is suitable for running the update utility under a periodic task scheduler such as the UNIX cron daemon or the Windows Task Scheduler. The Update Frequency setting is not applicable, as the scheduler determines the effective

frequency of updates. This is the recommended method of running the Secure Endpoint Update Server.

Linux Cron

The MIRRORDIR setting must specify a location that the update utility is able to write to.

```
./update-linux-[i386 or x86-64] fetch --once --config config.xml -
-mirror MIRRORDIR
```

For example, to update TETRA definitions hourly you would add the following to your crontab file:

```
0 * * * * [Full path to binary]/update-linux-[i386 or x86-64]
fetch --once --config [Full path to config]/config.xml - -mirror
MIRRORDIR
```

Windows Scheduled Task

The following set of instructions assumes that the Secure Endpoint Update Server has been installed with the following directory structure:

C:\AMP

C:\AMP\update-win-x86-64.exe

C:\AMP\config.xml

C:\AMP\mirror

We also assume that the utility will run once an hour every day in fetch mode.

1. Start the Task Scheduler.
2. Select **Create New Task**.
3. Select the **General** tab.
   - Enter a **Name** for the task.
   - Select **Run whether user is logged on or not**.
   - Select your operating system from the **Configure for** drop down.
4. Select the **Triggers** tab.
   - Click **New**.
   - Select **On a schedule** from the **Begin the task** drop down.
   - Select **Daily** under **Settings**.
   - Check **Repeat task every** and select **1 hour** from the drop down.
   - Verify that **Enabled** is checked.
   - Click **Ok**.
5. Select the **Actions** tab.
   - Click **New**.
   - Select **Start a program** from the **Action** drop down.
   - Enter `C:\AMP\update-win-x86-64.exe` or `C:\AMP\update-win-i386.exe` in the **Program/script** field.
   - Enter `fetch --config C:\AMP\config.xml --once --mirror C:\AMP\mirror` in the **Add arguments** field.

- Enter `C:\AMP` in the **Start in** field.
- Click **Ok**.

6. Select the **Conditions** tab.
   - [Optional] Check the **Wake the computer to run this task** option.
7. Select the **Settings** tab.
   - Verify that **Do not start a new instance** is selected under **If the task is already running**.
   - Click **Ok**.
8. Enter the credentials for the account that will run the task.

Fetch-Only Periodic Update Mode

The update utility will fetch TETRA updates into the directory specified by the '--mirror' parameter. Superuser mode is not required, but the destination directory (`MIRRORDIR`) must be writable by the user account that is executing the update utility. A third-party HTTP server, such as Apache or Nginx is required to host the TETRA updates for the Secure Endpoint Windows connectors. MIRRORDIR is the directory where your updates will be stored.

Linux hosts

```
./update-linux-[i386 or x86-64] fetch --config config.xml --mirror
MIRRORDIR
```

Windows hosts

```
update-win-[i386 or x86-64] fetch --config config.xml --mirror
MIRRORDIR
```

Self-Hosting Mode

In this mode, the Secure Endpoint Update Server will periodically download TETRA definitions and microdefinitions from the Secure Endpoint servers to a user-specified location, and host them using the built-in HTTP server. The self-hosting mode is only recommended for Proof-of-Concept, or small deployments. The user is responsible for the monitoring of the Secure Endpoint Update Server.

Self-Hosting Periodic Fetch Mode

The Secure Endpoint Update Server has to be run in superuser mode, as binding to privileged HTTP ports is required. In all cases below, the "MIRRORDIR" setting refers to a location specified by the end-user of the utility that will receive the updates and the configuration file setting (--config) can be omitted if the configuration file is placed in the same location as the update script.

Linux hosts

```
./update-linux-[i386 or x86-64] host --config config.xml --mirror
MIRRORDIR --server IPADDRESS
```

Windows hosts

```
update-win-[i386 or x86-64] host --config config.xml --mirror
MIRRORDIR --server IPADDRESS
```

Set up a Third-Party Web Server to Host the Content

Note that the Secure Endpoint connector requires the presence of the **Server** HTTP Header in the response for proper operation. If the **Server** HTTP Header has been disabled, the Web server may need additional configuration specified below.

Apache

```
RedirectMatch ^/av64bit_[\d]+/(.*) /av64bit/$1
RedirectMatch ^/av32bit_[\d]+/(.*) /av32bit/$1
```

Nginx

The following should be added to the “server” section of the configuration file:

```
rewrite ^/av64bit_[\d]+/(.*)$ /av64bit/$1 permanent;
rewrite ^/av32bit_[\d]+/(.*)$ /av32bit/$1 permanent;
```

Microsoft IIS

The url-rewrite extension must be installed. Add the following XML snippet to the server configuration at `/[MIRROR_DIRECTORY]/web.config`:

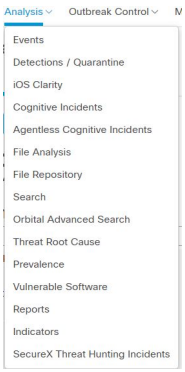
```
        <rewrite>
            <rules>
                <rule name="Rewrite fetch URL">
                    <match url="^(.*)_[\d]*\/avx\/(.*)$" />
                    <action type="Redirect" url="{R:1}/avx/{R:2}"
appendQueryString="false" />
                </rule>
            </rules>
        </rewrite>
```

Chapter 30
Talos Threat Hunting

Secure Endpoint Premier subscriptions include Cisco Talos Threat Hunting. Talos Threat Hunting leverages the expertise of both Talos and the Cisco Efficacy Research Team to help identify threats found in your environment. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. Once threats are detected, customers are notified so they can begin remediation.

Access Talos Threat Hunting

When Talos Threat Hunting has been enabled on your Secure Endpoint account you can access it from the Analysis menu.



There will also be an icon in the top right corner of the Console. A badge will be displayed showing the number of new incidents if any.

Any incidents will also appear in the Dashboard Tab and Events Tab as well as the Device Trajectory for any computers involved in the incident. Each event links to the Talos Threat Hunting Incident Report.

Overview

The overview pane provides comparative information between your organization and global data as well as the types of threat hunts performed.

Threat Hunt Overview

The Threat Hunt overview compares your organization to global incidents over the last 30 days. It is broken down into three categories:

- Potential threats – the number of raw events that the threat hunting team is examining.
- Cases – the potential threat events that trigger one of the Threat Hunt Types and require further examination.
- Confirmed threat – the cases that result in a confirmed threat to an organization.

Threat Hunt Types

Threat Hunt types are the average daily number of hunts conducted for your organization over the last 30 days. There are three types of threat hunts:

- Tactics & techniques – behavior-based threat hunts that are triggered by events showing the use of a specific set of tools, exploits, or a sequence of events that matches other compromise incidents.
- Intelligence – threat hunts based on current events or malware incidents taking place across the globe. These can also include threat hunts based on recently published vulnerabilities.
- Anomaly driven – threat hunts triggered by events that occur outside of expected activity. For example, a user logging in outside of their normal work hours or from a country they've never logged in from before.

Talos Threat Hunting Incidents

The Talos Threat Hunting Incidents page shows a list of incidents discovered through analysis of your organization's data.

Each report shows:

- the date and time it was created,
- the name of the incident as assigned by the analyst,
- any tactics and techniques employed,
- and the number of computers in your organization that were affected.

Click on the name of the incident to view the report.

Talos Threat Hunting Incident Report

Each Incident Report is custom-written to provide actionable information about the incident as well as remediation and mitigation steps where possible.

Incident Report Overview

The overview contains information about the incident at a glance.

Incident Started at is the time the analyst believes the incident started based on the available data. This time could be updated as more information is uncovered.

Incident Discovered on is the time the analyst first uncovered evidence that the incident took place.

The Tactics and Techniques include information from the MITRE ATT&CK knowledge base. Tactics represent the objective of an attack, such as executing malware or exfiltrating confidential information. Techniques are the methods attackers use to achieve the objectives or what they gain. For more information, see Getting Started with ATT&CK.

Summary provides details the analyst uncovered about the incident from observing data from your Secure Endpoint account as well as other Cisco XDR or SecureX products you use. Methods, objectives, and other significant details involved in the incident will be included to provide context.

Remediation includes recommendations on actions that can or should be taken, to include pointed investigation components from the incident. Any possible mitigation measures for the specific incident may be included if applicable.

Orbital Queries provides any existing and custom Orbital queries that you can use to gather additional information and evidence about the incident.

Incident Report Computers

This section shows a list of computers from your Secure Endpoint deployment that were involved in the incident. This allows you to easily view the Device Trajectory and Events associated with the involved computers and go directly to policies used by the connectors to make changes.

Incident Report Timeline

This shows a detailed execution chain that covers the Secure Endpoint connector events associated with the incident.

Appendix A
Threat Descriptions

Secure Endpoint 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.

File Disposition

Files observed by your connectors are divided into three disposition types:

- Clean – the file is known to be clean or signed with a trusted certificate.
- Malicious – the file is known malware or harmful.
- Unknown – there is insufficient data to make a determination.

Indications of Compromise

Secure Endpoint calculates devices with Trajectory Indications of Compromise based on events observed over the last 7 days. A single Cloud IOC will only be reported once every four hours per endpoint. 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.
- Global threat alert – global threat alerts 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 global threat alert indication of compromise event is generated when suspicious or anomalous traffic is detected in your organization. Only threats that global threat alerts has assigned a severity of 7 or higher are sent to Secure Endpoint.

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 – Allowed Applications.

Device Flow Correlation Detections

Device flow correlation allows you to flag or block suspicious network activity. You can use Policies to specify Secure Endpoint Secure Endpoint 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. Device flow correlation detections include:

- DFC.CustomIPList – The computer made a connection to an IP address you have defined in a device flow correlation IP blocked 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.

IMPORTANT! Device flow correlation is incompatible with applications that do network tunneling, like VPN.

Appendix B
Connector Firewall Exceptions

To allow the Secure Endpoint connectors 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. All connectors – Windows, Mac, Linux, Android, and iOS – require access to certain servers while others are only required if certain features are enabled.

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

North America Firewall Exceptions

All connectors for organizations located in North America require 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.amp.cisco.com
- **Remote File Fetch** – rff.amp.cisco.com
- **Connector Upgrades** – upgrades.amp.cisco.com (TCP 80 and 443)

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

- **Cloud Host for Windows, Mac, and Linux** – cloud-ec-asn.amp.cisco.com
- **Cloud Host for iOS** – cloud-ios-asn.amp.cisco.com

- **Cloud Host for Android** – cloud-android-asn.amp.cisco.com
- **Enrollment Server** – enrolment.amp.cisco.com

To use Orbital on your Windows, Mac, and Linux connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** – orbital.amp.cisco.com
- **Orbital Queries** – ncp.orbital.amp.cisco.com
- **Orbital Installer** – update.orbital.amp.cisco.com

If you have the Behavioral Protection feature enabled on your Windows, Mac, and Linux connectors you need to allow access to the following server over TCP 443 for signature updates:

- **Behavioral Protection Signatures** – apde.amp.cisco.com

If you have TETRA enabled on any of your Secure Endpoint Windows connectors you must allow access to the following servers over TCP 80 and 443 for signature updates:

- **Update Server** – tetra-defs.amp.cisco.com
- **Certificate Validation** – commercial.ocsp.identrust.com, validation.identrust.com

If you have Device Control enabled on any of your Secure Endpoint Windows connectors you must allow access to the following servers over TCP 443:

- **Device Control** – endpoints.amp.cisco.com

If you use the Endpoint IOC Scanner on your Secure Endpoint Windows connectors you must allow access to the following server over TCP 443:

- **Endpoint IOC Downloads** – ioc.amp.cisco.com

If you have any Custom Detections – Advanced signatures you want your endpoints to use you must allow access to the following server over TCP 443:

- **Advanced Custom Signatures** – custom-signatures.amp.cisco.com

European Union Firewall Exceptions

All connectors for organizations located in the European Union must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **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.cisco.com
- **Remote File Fetch** – rff.eu.amp.cisco.com
- **Connector Upgrades** – upgrades.eu.amp.cisco.com (TCP 80 and 443)

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

- **Cloud Host for Windows, Mac, and Linux** – cloud-ec-asn.eu.amp.cisco.com
- **Cloud Host for iOS** – cloud-ios-asn.eu.amp.cisco.com
- **Cloud Host for Android** – cloud-android-asn.eu.amp.cisco.com
- **Enrollment Server** – enrolment.eu.amp.cisco.com

To use Orbital on your Windows, Mac, and Linux connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.eu.amp.cisco.com
- **Orbital Queries** - ncp.orbital.eu.amp.cisco.com
- **Orbital Installer** - update.orbital.eu.amp.cisco.com

If you have the Behavioral Protection feature enabled on your Windows, Mac, and Linux connectors you need to allow access to the following server over TCP 443 for signature updates:

- **Behavioral Protection Signatures** - apde.eu.amp.cisco.com

If you have TETRA enabled on any of your Secure Endpoint Windows connectors you must allow access to the following servers over TCP 80 and 443 for signature updates:

- **Update Server** - tetra-defs.eu.amp.cisco.com
- **Certificate Validation** - commercial.ocsp.identrust.com, validation.identrust.com

If you have Device Control enabled on any of your Secure Endpoint Windows connectors you must allow access to the following servers over TCP 443:

- **Device Control** - endpoints.eu.amp.cisco.com

If you use the Endpoint IOC Scanner you must allow access to the following server over TCP 443:

- **Endpoint IOC Downloads** - ioc.eu.amp.cisco.com

If you have any Custom Detections - Advanced signatures you want your endpoints to use you must allow access to the following server over TCP 443:

- **Advanced Custom Signatures** - custom-signatures.eu.amp.cisco.com

Asia Pacific, Japan, and Greater China Firewall Exceptions

All connectors for organizations located in Asia Pacific, Japan, and Greater China must allow connectivity from the connector to the following servers over HTTPS (TCP 443):

- **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.cisco.com
- **Remote File Fetch** - rff.apjc.amp.cisco.com
- **Connector Upgrades** - upgrades.apjc.amp.cisco.com (TCP 80 and 443)

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

- **Cloud Host for Windows, Mac, and Linux** - cloud-ec-asn.apjc.amp.cisco.com
- **Cloud Host for iOS** - cloud-ios-asn.apjc.amp.cisco.com
- **Cloud Host for Android** - cloud-android-asn.apjc.amp.cisco.com
- **Enrollment Server** - enrolment.apjc.amp.cisco.com

To use Orbital on your Windows, Mac, and Linux connectors, you must allow access to the following servers over TCP 443:

- **Orbital Updates** - orbital.apjc.amp.cisco.com
- **Orbital Queries** - ncp.orbital.apjc.amp.cisco.com
- **Orbital Installer** - update.orbital.apjc.amp.cisco.com

If you have the Behavioral Protection feature enabled on your Windows, Mac, and Linux connectors you need to allow access to the following server over TCP 443 for signature updates:

- **Behavioral Protection Signatures** - apde.apjc.amp.cisco.com

If you have TETRA enabled on any of your Secure Endpoint Windows connectors you must allow access to the following servers over TCP 80 and 443 for signature updates:

- **Update Server** - tetra-defs.apjc.amp.cisco.com
- **Certificate Validation** - commercial.ocsp.identrust.com, validation.identrust.com

If you have Device Control enabled on any of your Secure Endpoint Windows connectors you must allow access to the following servers over TCP 443:

- **Device Control** - endpoints.apjc.amp.cisco.com

If you use the Endpoint IOC Scanner you must allow access to the following server over TCP 443:

- **Endpoint IOC Downloads** - ioc.apjc.amp.cisco.com

If you have any Custom Detections - Advanced signatures you want your endpoints to use you must allow access to the following server over TCP 443:

- **Advanced Custom Signatures** - custom-signatures.apjc.amp.cisco.com

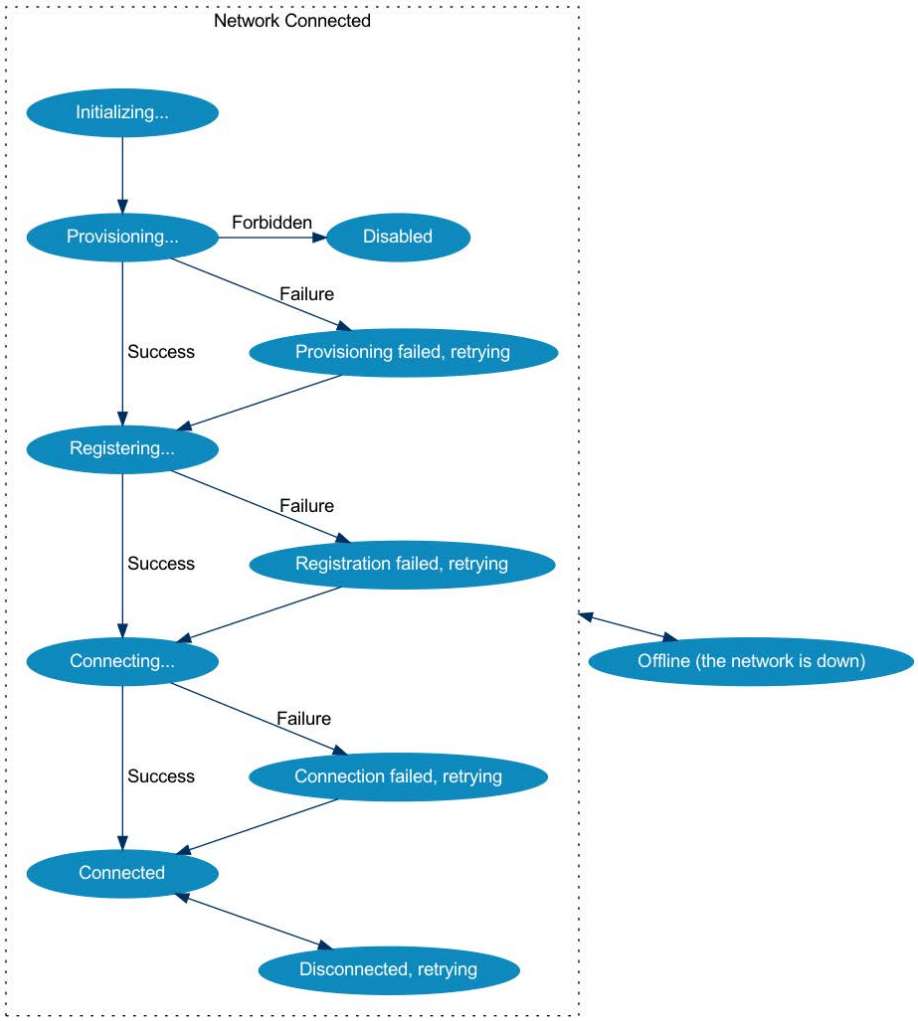
Appendix C
Mac/Linux Connector Status

The Secure Endpoint Mac and Linux connectors report a status that represents a combination of the following:

- Endpoint Identity Enrollment/Subscription
- Endpoint Identity Registration
- Disposition Service Registration
- Secure Endpoint Service Connection
- Network Status

The status is displayed in the Secure Endpoint Mac connector UI and can also be accessed through ampcli on both Mac and Linux using the `/opt/cisco/amp/ampcli status` command.

This diagram outlines the general flow of the connection process and status.


Network Connected
Initializing...
Provisioning...
Forbidden
Disabled
Failure
Success
Provisioning failed, retrying
Registering...
Failure
Success
Registration failed, retrying
Connecting...
Offline (the network is down)
Failure
Success
Connection failed, retrying
Connected
Disconnected, retrying

Appendix C

This table describes how the status indicator is set.

STATUS	DESCRIPTION	REASONS
Initializing...	Program starting/loading.	N/A
Provisioning...	Endpoint identity enrollment/subscription.	N/A
Provisioning failed, retrying...	Endpoint identity enrollment/subscription failed. Connector will retry.	Cannot reach Secure Endpoint services. Missing SSL certificates.
Registering...	Registering endpoint identity.	N/A
Registration Failed, retrying...	Endpoint identity registration failed. connector will retry.	Cannot reach Secure Endpoint services. Missing SSL certificates.
Connecting...	Registering with disposition service.	N/A
Connection failed, retrying...	Registration with disposition service failed. connector will retry.	Cannot reach Secure Endpoint services. Missing SSL certificates.
Connected	Enrollment and registration succeeded. Connected to Secure Endpoint services. connector is operating normally.	N/A
Disabled	connector is not operational.	Secure Endpoint subscription is invalid or has expired.
Disconnected, retrying...	Lost connection to the disposition service after an initial connection was established. connector will attempt to reconnect.	Network connection to the disposition service has been interrupted.
Offline (the network is down)	The local network has been disconnected.	Cable disconnected. The network interface is disabled.

Appendix D
Supporting Documents

The following supporting documents are available for download.

Cisco Secure Endpoint User Guide

The current version of the User Guide can be downloaded here.

Download the User Guide

Cisco Secure Endpoint Quick Start Guide

This guide walks through setting up groups, policies, and exclusions then deploying Secure Endpoint connectors. This guide is useful for evaluating Secure Endpoint.

Download the Quick Start Guide

Cisco Secure Endpoint Deployment Strategy Guide

This guide provides a more detailed look at preparing and planning for a production deployment of Secure Endpoint along with best practices and troubleshooting tips.

Download the Deployment Strategy Guide

Cisco Secure Endpoint Support Documentation

TechNotes for configuring, maintaining, and troubleshooting Secure Endpoint.

Support Documentation

Cisco Endpoint IOC Attributes

The Endpoint IOC Attributes document details IOC attributes supported by the Endpoint IOC scanner included in the Secure Endpoint connector. Sample IOC documents that can be uploaded to your Secure Endpoint console are also included.

Download the Endpoint IOC Attributes

Cisco Secure Endpoint API Documentation

The API allows you to access your Secure Endpoint data and events without logging into the console. The documentation provides descriptions of available interfaces, parameters, and examples.

View the API documentation

Cisco Secure Endpoint Release Notes

The Release Notes contain the Secure Endpoint change log.

Download the Release Notes

Cisco Secure Endpoint Demo Data Stories

The Demo Data stories describe some of the samples that are shown when Demo Data is enabled in Secure Endpoint.

Download the Device Control document

Download the WMIPRVSE document

Download the FriedEx document

Download the WannaCry Ransomware document

Download the Cognitive Threat Analytics (CTA) document

Download the Command Line Capture document

Download the Low Prevalence Executable document

Download the Cryptowall document

Download the PlugX document

Download the Upatre document

Download the CozyDuke document

Download the SFEICAR document

Download the ZAccess document

Download the ZBot document

Cisco Universal Cloud Agreement

Cloud Offer Terms

Index

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z