## Table of Contents

### Chapter 1: Dashboard
- System Requirements ................................................................. 7
- Menu ........................................................................................................... 7
  - Dashboard ........................................................................................................ 7
  - Analysis ........................................................................................................... 8
  - Outbreak Control .......................................................................................... 9
  - Reports ......................................................................................................... 9
  - Management ............................................................................................... 10
  - Accounts ..................................................................................................... 10
- Overview Tab ........................................................................................................... 11
  - Indications of Compromise ............................................................................. 11
  - Malware and Network Threat Detections .................................................... 13
- Events Tab ............................................................................................................... 13
  - Filters and Subscriptions ............................................................................ 13
  - SHA-256 File Info Context Menu ................................................................. 14
  - List View .................................................................................................... 15
- Heat Map Tab .......................................................................................................... 16

### Chapter 2: Outbreak Control
- Custom Detections - Simple .................................................................................... 18
- Custom Detections - Advanced ............................................................................... 19
- Application Control - Blocking ................................................................................. 21
- Application Control - Whitelisting ............................................................................ 22
- Network - IP Blacklists & Whitelists ......................................................................... 23
  - IP Blacklists ................................................................................................ 23
  - IP Whitelists ................................................................................................. 24
  - Editing IP Blacklists and Whitelists .............................................................. 25

### Chapter 3: Exclusions
- Creating and Managing Exclusions ........................................................................... 26
- Antivirus Compatibility Using Exclusions ................................................................. 28
  - Creating Antivirus Exclusions in the FireAMP Connector ......................... 28
  - Creating Exclusions for the FireAMP Connector in Antivirus Software ... 29

### Chapter 4: Policies
- Policy Contents ........................................................................................................... 33
  - Name, Lists, and Description ........................................................................... 33
### Table of Contents

**FireAMP Windows Connector**  ................................................................. 35  
  - General Tab ..................................................................................... 35  
  - File Tab ............................................................................................ 40  
  - Network Tab ................................................................................... 45  

**FireAMP Mac Connector** ................................................................. 46  
  - General Tab ..................................................................................... 46  
  - File Tab ............................................................................................ 48  
  - Network Tab ................................................................................... 51  

**FireAMP Linux Policy** ................................................................. 52  
  - General Tab ..................................................................................... 52  
  - File Tab ............................................................................................ 54  
  - Network Tab ................................................................................... 57  

**Chapter 5: Groups** .............................................................................. 59  
  - Configuring the Group ................................................................. 59  
    - Name and Description .............................................................. 60  
    - Parent Menu ............................................................................... 60  
    - Policy Menu ............................................................................... 60  
    - Child Groups ............................................................................. 60  
  - Adding and Moving Computers .................................................. 60  

**Chapter 6: Deploying the FireAMP Connector** .............................. 61  
  - Download Connector ................................................................. 61  
    - FireAMP Windows Connector .................................................... 61  
    - FireAMP Mac Connector ............................................................ 62  
    - FireAMP Linux Connector .......................................................... 62  
  - Deployment Summary ................................................................. 63  
  - Computer Management ................................................................. 63  

**Chapter 7: FireAMP Windows Connector** ...................................... 65  
  - System Requirements .................................................................. 65  
  - Previously Supported Versions .................................................... 66  
  - Incompatible software and configurations .................................. 67  
  - Firewall Connectivity ................................................................. 67  
    - Firewall Exceptions ................................................................. 67  
    - European Union Firewall Exceptions ........................................ 68  
  - Proxy Autodetection ................................................................. 68  
  - Installer ......................................................................................... 69  
    - Interactive Installer ................................................................. 69  
    - Installer Command Line Switches ............................................ 72  
    - Installer Exit Codes ................................................................. 73  
  - Connector User Interface ............................................................ 73  
    - Scanning ..................................................................................... 74  
    - History ....................................................................................... 75  
    - Settings ..................................................................................... 75
# Table of Contents

Uninstall................................................................................................................... 76

## Chapter 8: FireAMP Mac Connector.......................................... 78
- System Requirements ....................................................................................... 78
- Previously Supported Versions .................................................................... 78
- Incompatible Software and Configurations.................................................... 79
- Firewall Connectivity...................................................................................... 79
  - Firewall Exceptions...................................................................................... 79
  - European Union Firewall Exceptions ......................................................... 80
- Installing the FireAMP Mac Connector ............................................................ 80
- Using the FireAMP Mac Connector ................................................................. 81
  - Settings....................................................................................................... 82
  - Mail.app..................................................................................................... 82
- Uninstall............................................................................................................ 82

## Chapter 9: FireAMP Linux Connector ........................................ 84
- System Requirements....................................................................................... 84
- Previously Supported Versions .................................................................... 85
- Incompatible Software and Configurations.................................................... 85
- Firewall Connectivity...................................................................................... 85
  - Firewall Exceptions...................................................................................... 86
  - European Union Firewall Exceptions ......................................................... 86
- Installing the FireAMP Linux Connector .......................................................... 86
- Connector Updates .......................................................................................... 87
- Using the FireAMP Linux Connector ............................................................... 87
- Support Tool..................................................................................................... 87
- Uninstall............................................................................................................ 87

## Chapter 10: Endpoint IOC Scanner ............................................. 89
- Installed Endpoint IOCs.................................................................................... 89
  - Uploading Endpoint IOCs ............................................................................ 89
  - View and Edit ............................................................................................... 90
  - Activate Endpoint IOCs ............................................................................... 90
- Initiate Scan...................................................................................................... 90
  - Scan by Policy............................................................................................... 91
  - Scan by Computer......................................................................................... 92
- Scan Summary .................................................................................................. 92

## Chapter 11: Search..................................................................... 94
- Hash Search...................................................................................................... 94
- String Search................................................................................................... 95
- Network Activity Searches............................................................................. 96
Chapter 12: File Analysis ................................................................. 97
  File Analysis Landing Page ................................................................. 97
  Threat Analysis ............................................................................... 98
    Metadata ......................................................................................... 99
    Behavioral Indicators ....................................................................... 99
    HTTP Traffic .................................................................................. 102
    DNS Traffic ................................................................................... 102
    TCP/IP Streams ............................................................................. 102
    Processes ......................................................................................... 103
    Artifacts .......................................................................................... 103
    Registry Activity ............................................................................ 104
    Filesystem Activity ......................................................................... 104

Chapter 13: Trajectory ............................................................................. 105
  File Trajectory ................................................................................... 105
    Description ..................................................................................... 105
  Device Trajectory .............................................................................. 110
    Description ..................................................................................... 110
    Indications of Compromise ................................................................. 111
    Filters and Search ........................................................................... 112

Chapter 14: File Repository............................................................... 114
  Requesting a remote file .................................................................... 115

Chapter 15: Threat Root Cause......................................................... 118
  Select Dates ..................................................................................... 118
  Overview .......................................................................................... 118
  Details ................................................................................................ 119
  Timeline ............................................................................................. 120

Chapter 16: Prevalence .......................................................................... 122
  Low Prevalence Executables ................................................................. 122
    Automatic Analysis .......................................................................... 123

Chapter 17: Vulnerable Software .......................................................... 124
  Common Vulnerabilities and Exposures .............................................. 125
  Common Vulnerability Scoring System .............................................. 125
  Additional Information on Vulnerable Software .................................. 126
## Chapter 18: Reports

- Creating a Report ................................................................. 128
- Report Sections ................................................................. 128

## Chapter 19: Accounts

- Users ...................................................................................... 130
  - Time Zone Settings .............................................................. 131
  - Access Control ................................................................. 132
  - Two-Step Verification ....................................................... 135
- API Credentials ................................................................. 137
- Business ............................................................................... 138
  - Features ........................................................................... 139
- Audit Log .............................................................................. 140
- Demo Data ........................................................................... 141
- Applications .......................................................................... 142
  - Application Settings ....................................................... 142
  - Edit an Application ....................................................... 143

## Appendix A: Threat Descriptions

- Indications of Compromise ................................................... 144
- DFC Detections ...................................................................... 145

## Appendix B: Supporting Documents

- Cisco FireAMP Private Cloud Console User Guide .................. 146
- Cisco FireAMP Private Cloud User Guide .............................. 146
- Cisco FireAMP Private Cloud Quick Start Guide .................... 146
- Cisco FireAMP Private Cloud Deployment Strategy Guide .......... 146
- Cisco Endpoint IOC Attributes ........................................... 147
- Cisco FireAMP Private Cloud Release Notes .......................... 147
- Cisco FireAMP Demo Data Stories ........................................ 147
The FireAMP Dashboard gives you a quick overview of trouble spots on devices in your environment along with updates about malware and network threat detections. From the dashboard page you can drill down on events to gather more detailed information and remedy potential compromises.
System Requirements

To access the FireAMP Console you will need one of the following Web browsers:

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

Menu

The menu bar at the top indicates the total number of installs and the number of malware detections in the last 7 days. The current number of system announcements is also shown at the top of the page along with a link to view previous announcements. Menu items take you to the Dashboard, Analysis, Outbreak Control, Reports, Management, and Accounts as indicated below. It also has a link to contact Support, the Help system and a Logout link to end your session. The My Account link will take you directly to the Users page for your account so you can make changes.

IMPORTANT! The global Group Filter is persistent even if you log out of the FireAMP Console and log in again.

Dashboard

The Dashboard link takes you back to the dashboard which contains different widgets highlighting events in your environment requiring attention.
Analysis

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

- **Events Tab** to view raw events from Connectors.
- **Detections / Quarantine** to view any detections and items that were quarantined.
- **File Analysis** to see in detail what a binary does.
- **File Repository** to download files retrieved from your FireAMP Connectors. (Administrator only)
- **Search** to find data from your FireAMP deployment.

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

- **Threat Root Cause** to see how malware is getting onto your computers.
- **Prevalence** to view files that have been executed in your deployment.
- **Vulnerable Software** to view applications with known vulnerabilities observed by the FireAMP Connector.
- **Reports** to view weekly reports about your FireAMP deployment.
Outbreak Control

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

- Custom Detections
  - Simple to convict files that are not yet classified.
  - Advanced to create signatures that will detect parts of the Portable Executable (PE) file.
- Application Control
  - Blocking to stop executables from running.
  - Whitelisting to create lists of applications that will not be wrongly detected.
- Network
  - IP Blacklists & Whitelists to explicitly detect or allow connections to specified IP addresses.
- Endpoint IOC
  - Initiate Scan to schedule and start IOC scans on your FireAMP Connectors. (Administrator only)
  - Installed Endpoint IOCs to upload new endpoint IOCs and view installed endpoint IOCs. (Administrator only)
  - Scan Summary to view the results of endpoint IOC scans.

Reports

The Reports link allows you to view previously created PDF reports based on your data. (Administrator only)
Dashboard Menu

Chapter 3

Management

The Management menu contains items that allow you to manage your FireAMP Connectors.

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

Accounts

The Accounts menu contains items related to FireAMP console accounts:

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

The Overview tab is composed of multiple widgets highlighting recent malicious activity in your FireAMP deployment. The tab is divided into three types of information: Indications of Compromise, malware detections, and network threats.

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

Indications of Compromise

The Indications of Compromise widget provides you with a list of potentially compromised devices in your FireAMP deployment and quick links to inspect activity.
to remedy the problem. After the issues have been addressed you can then mark it as resolved.

FireAMP calculates devices with Indications of Compromise based on events observed over the last 7 days. Events such as malicious file detections, a parent file repeatedly downloading a malicious file (Potential Dropper Infection), or multiple parent files downloading malicious files (Multiple Infected Files) are all contributing factors. Devices considered to be at the highest risk are displayed at the top of the list.

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

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

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

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

Events Tab

The Events tab initially shows the most recent events in your FireAMP 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

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

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

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

**SHA-256 File Info Context Menu**

Right-clicking on a SHA-256 in the FireAMP console will display a specific context menu that allows you to see additional information and perform several actions. The context menu displays the current disposition of the SHA-256 as well as the specific filename associated with it. You can also see how many vendors detect the file.
according to VirusTotal. The longest common name used for the file on VirusTotal is also displayed.

- 27d9820.3d352c
- Disposition: Malicious
- Filename: 0dfa700b33fc6b859e4de543937850a9.exe
- VirusTotal: [21 /47]
- Backdoor Full Report
- Copy SHA-256
- Search
- View Full SHA-256
- File Analysis
- File Trajectory
  - Simple Detection
  - Application Blocking
  - Whitelisting
- Back
- Forward
- Reload

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

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

**List View**

List View initially shows the name of the computer that had a detection, the name of the detection, most recent action taken, and the time and date of the event. Click on an event to view more detailed information on the detection, Connector info, and any comments about the event. In the detail 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.

**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 to entries with matching fields. You can also use the Export to CSV button to export the current filtered view to a CSV file to download.

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

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

**Heat Map Tab**

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

Clicking a Group in the Heat Map will take you to a filtered view of the Events Tab showing Threat Detected events for that group.
You can search for groups by name in the box at the bottom indicated by “Search the groups in the heat map”. This will white out the other groups and highlight the one you are searching for.

You can hover your pointer over a group and see the number of computers, detections in the last 7 days, and the mean detections per computer. The tree map refreshes hourly so changes may not always be immediately apparent.
FireAMP offers a variety of lists, classified as Outbreak Control, that allow you to customize it to your needs. The main lists are Simple Custom Detections, Application Blocking, Application Whitelists, Advanced Custom Detections, and IP Blacklists and Whitelists.

Custom Detections - Simple

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

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

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

You can add a single SHA-256 and create a note about the file. You can upload a file (up to 20MB) and the SHA-256 will be taken from the file and you can add a note, 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 added a SHA-
256 that you did not want to, you can click on **Remove**. You can also edit the name of the list and click **Save** to rename it.

Note that when you add a Simple Custom Detection that it is subject to caching. The length of time a file is cached depends on its disposition:
- Clean files - 7 days
- Unknown files - 1 hour
- Malicious files - 1 hour

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

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

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

---

**Custom Detections - Advanced**

Advanced Custom Detections are like traditional antivirus signatures, but they are written by the user. These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:
- MD5 Signatures
- MD5, PE section based Signatures
- File Body-based Signatures
- Extended Signature Format (offsets, wildcards, regular expressions)
- Logical Signatures
- Icon Signatures
More information on signature formats can be found at http://immunet-janus-helpdoc.s3.amazonaws.com/clamav_signatures.pdf. These signatures are compiled into a file downloaded to the endpoint.

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

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

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

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

Note that when you create an Advanced Custom Detection for a file that it is subject to caching. The length of time a file is cached for depends on its disposition:

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

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

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

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

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

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

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

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

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

If the file is already in your local cache you will have to wait until the cache expires before Application Blocking takes effect. The length of time a file is cached for depends on its disposition:
Clean files - 7 days
Unknown files - 1 hour
Malicious files - 1 hour

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

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

Application Control – Whitelisting

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

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

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

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

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

**Network - IP Blacklists & Whitelists**

IP Blacklists and Whitelists are used with Device Flow Correlation (DFC) to define custom IP address detections. After you have created your lists you can then define in policy to use them in addition to the Cisco Intelligence Feed or on their own.

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

For example if you add these entries to a list:

- 192.168.1.0/23
- 192.168.1.15
- 192.168.1.135
- 192.168.1.200

The list will be processed with a net result of:

- 192.168.1.0/23

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

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

The list will be processed with a net result of:

- 192.168.1.0/23
- 192.168.1.15:80

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

- 0.0.0.1/1:XX
- 128.0.0.1/1:XX

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

Click the View All Changes link to see the Audit Log with all records filtered to show only IP Blacklist & Whitelist entries. Click View Changes next to a single IP list to view the Audit Log with all records filtered to show only the records for that specific list.

**IP Blacklists**

An IP Black 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 a single IP address, an entire CIDR block, or specify an IP address and port number. When a computer makes a connection to an IP address in your list the action taken depends on what you have specified in the Network > Device Flow Correlation (DFC) section of your policy.
To create an IP Black List go to Outbreak Control > IP Blacklists & Whitelists and click Create IP List. Give the list a name and select Blacklist from the List Type pull down. You can then either enter IP addresses, CIDR blocks, or IP address and port combinations in the field provided or upload a text file containing the addresses you want blocked. Once you have entered the addresses or uploaded your list, click Create IP List to save the list.

### IP Whitelists

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

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

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

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

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

WARNING! Any files located in a directory that has been added to an Exclusion list will not be subjected to Application Blocking, Simple Custom Detections, or Advanced Custom Detection lists.

Creating and Managing Exclusions

To create a Custom Exclusion Set, go to Management > Exclusions. Click Create Exclusion Set, select whether the exclusions will be for FireAMP Windows or FireAMP Mac Connectors, give it a name, and click Create.
After you save the Exclusion Set, click **Edit** and you will see an **Add Exclusion** link. Clicking the **Add Exclusion** link will bring up a modal dialog box.

![New Exclusion dialog box](image)

You can add a Path, Threat name, File Extension, or use wild cards for file names, extensions, or paths, and then click **Create**.

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

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

**IMPORTANT!** The CSIDLs are case sensitive.

Path exclusions are the most frequently used since 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
```

**TIP!** You do not need to escape "space" characters in a path.

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

```
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
```

**IMPORTANT!** Path exclusions will prevent the FireAMP Connector from scanning all files and subdirectories in the directory specified.

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

/Users/johndoe/Documents/Virtual Machines/

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

/Users/*/Documents/Virtual Machines/

If you accidentally create an exclusion you do not want, you can click on the Edit button to expand the exclusion set, then select the specific exclusion and click Delete. Click View All Changes to see a filtered list of the Audit Log showing all Exclusion Set changes or click View Changes on a specific Exclusion Set to see changes made to just that particular set.

Antivirus Compatibility Using Exclusions

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

Creating Antivirus Exclusions in the FireAMP Connector

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

Repeat this procedure for each path associated with your security applications.

Common CSIDLs for security products that should be excluded are:

**Kaspersky**
- CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data

**McAfee VirusScan Enterprise**
- CSDL_PROGRAM_FILES\McAfee
- CSDL_PROGRAM_FILES\\McAfee
- CSDL_PROGRAM_FILES\Common Files\McAfee
- CSDL_COMMON_APPDATA\McAfee
- CSDL_PROGRAM_FILES\VSE
- CSDL_COMMON_APPDATA\VSE
- CSDL_PROGRAM_FILES\Common Files\VSE
Microsoft ForeFront
- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILES\X86\Microsoft Forefront

Microsoft Security Client
- CSIDL_PROGRAM_FILES\Microsoft Security Client
- CSIDL_PROGRAM_FILES\X86\Microsoft Security Client

Sophos
- CSIDL_PROGRAM_FILES\Sophos
- CSIDL_PROGRAM_FILES\X86\Sophos
- CSIDL_COMMON_APPDATA\Sophos\Sophos Anti-Virus\n
Splunk
- CSIDL_PROGRAM_FILES\Splunk

Symantec Endpoint Protection
- CSIDL_COMMON_APPDATA\Symantec
- CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection
- CSIDL_PROGRAM_FILES\X86\Symantec\Symantec Endpoint Protection

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

Creating Exclusions for the FireAMP Connector in Antivirus Software

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

Creating Exclusions for the FireAMP Connector in McAfee ePolicy Orchestrator 4.6

1. Log in to ePolicy Orchestrator.
2. Select Policy >Policy Catalog from the Menu.
3. Select the appropriate version of VirusScan Enterprise from the Product pulldown.
5. Select the Exclusions tab click the Add button.
6. In the By Pattern field enter the path to your FireAMP Connector install (C:\Program Files\Sourcefire by default) and check the Also exclude subfolders box.

**IMPORTANT!** You should exclude the FireAMP Connector using the Sourcefire directory as other files and sub-folders

7. Click OK.
8. Click Save.
10. Repeat steps 5 through 8 for this policy.

Creating Exclusions for the FireAMP Connector in McAfee VirusScan Enterprise 8.8

1. Open the VirusScan Console.
3. Select All Processes from the left pane.
4. Select the Exclusions tab.
5. Click the Exclusions button.
6. On the Set Exclusions dialog click the Add button.
7. Click the Browse button and select your FireAMP Connector install directory (C:\Program Files\Sourcefire by default) and check the Also exclude subfolders box.
8. Click OK.
9. Click OK on the Set Exclusions dialog.

Creating Exclusions for the FireAMP Connector in a Managed Symantec Enterprise Protection 12.1 Install

1. Log into Symantec Endpoint Protection Manager.
2. Click Policies in the left pane.
3. Select the Exceptions entry under the Policies list.
4. You can either add a new Exceptions Policy or edit an existing one.
5. Click Exceptions once you have opened the policy.
6. Click the Add button, select Windows Exceptions from the list and choose Folder from the submenu.
7. In the Add Security Risk Folder Exception dialog choose [PROGRAM_FILES] from the Prefix variable dropdown menu and enter Sourcefire in the Folder field. Ensure that Include subfolders is checked.
8. Under Specify the type of scan that excludes this folder menu select All.
9. Click OK.

10. Make sure that this Exception is used by all computers in your organization with the FireAMP Connector installed.

Creating Exclusions for the FireAMP Connector in an Unmanaged Symantec Enterprise Protection 12.1 Install

1. Open SEP and click on Change Settings in the left pane.
2. Click Configure Settings next to the Exceptions entry.
3. Click the Add button on the Exceptions dialog.
4. Select Folders from the Security Risk Exception submenu.
5. Select your FireAMP Connector installation directory (C:\Program Files\Sourcefire\FireAMP by default) from the dialog and click OK.
6. Click the Add button on the Exceptions dialog.
7. Select Folder from the SONAR Exception submenu.
8. Select your FireAMP Connector installation directory (C:\Program Files\Sourcefire\FireAMP by default) from the dialog and click OK.
9. Click the Close button.

Creating Exclusions for the FireAMP Connector in Microsoft Security Essentials

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

**IMPORTANT!** Because the process exclusions in Microsoft Security Essentials require a specific path to the sfc.exe file you will need to update this exclusion whenever you upgrade to a new version of the FireAMP Connector.
Outbreak Control and Exclusions lists are combined with other settings into a policy. The policy affects the behavior and certain settings of the FireAMP Connector. A policy is applied to a computer via Groups.

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

This will take you to the creation page. The configuration is covered below.
There are numerous settings that can be set in the policy. This section will detail each one. FireAMP Windows and FireAMP Mac both share some basic policy settings.

Name, Lists, and Description

The Name is just a name that you can use to recognize the policy. Select the lists you want to assign to the policy. See Custom Detections - Simple, Custom Detections - Advanced, Application Control - Blocking, Application Control - Whitelisting, Network.
- IP Blacklists & Whitelists, and Exclusions for details on creating these lists. The description can be used to give more description about the policy.

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

When you click IP Blacklists & Whitelists Edit button a dialog appears to select your lists.

Select the list you want to add from the pull down and click Add. You can add multiple IP lists to a single policy, however IP Whitelist entries will override IP Blacklist entries.
FireAMP Windows Connector

This section describes the Policy options that are available for FireAMP Windows Connectors. The options are divided into three tabs - General, File, and Network.

General Tab

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

General > Administrative Features

- **Send User Name in Events** will send the actual user name that the process is executed, copied, or moved as if known. This is useful for tracking down who is seeing malware. If this is not enabled, you will see a “u” for malware executed, copied, or moved as a user and “a” for something executed copied or moved as an administrator.
- **Send Filename and Path Info** will send the filename and path information to FireAMP so that they are visible in the Events Tab, Device Trajectory, and File Trajectory. Unchecking this setting will stop this information from being sent.
- **Heartbeat Interval** is the interval in which the Connector calls home to see if there are any files to restore via Cloud Recall™ 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.
- **Connector Protection** allows you to require a password to uninstall the FireAMP Connector or stop its service. This setting only applies to version 3.1.0 and higher of the FireAMP Connector.
- **Connector Protection Password** is the password you supply to Connector Protection to stop the FireAMP Connector service or uninstall it.

**IMPORTANT!** If you enable Connector Protection on a policy that includes previously deployed Connectors, you must reboot the computer or stop and restart the Connector service for this setting to take effect.
Automated Crash Dump Uploads allows you to choose whether to automatically upload FireAMP Connector crash dump files to Cisco for analysis.

General > Product Updates

When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the Product Version showing which version you are going to and it will populate the Update Server so you can see where the files will be pulled from. There will also be information to show how many Connectors in Groups that use the policy will require a reboot after updating. You can then configure the Start Update Window and End Update Window. The Update Interval allows you to specify how long your Connectors will wait between checks for new product updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic.

Start Update Window allows you to choose a date and time in which the updates can start occurring.
**End Update Window** allows you to choose a date and time in which the updates will stop occurring.

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

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

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

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

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

The **Reboot** behavior still includes **Do not reboot** and **Ask for reboot**, but you can also select **Force reboot after...** and specify the **Reboot Delay**. This value can be set to 2 minutes, 10 minutes, or 30 minutes.
**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 FireAMP Connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud. **Verbose Notifications** are boxes that pop-up from the Windows system tray that tell the user when they are copying a trusted file. This should be turned off unless troubleshooting. **Hide File Notifications** suppresses notifications from being displayed to the user when a malicious file is convicted or quarantined by the Connector. **Hide Cataloging Notifications** suppresses notifications to the user about cataloging before full endpoint IOC scans. **Hide Network Notifications** suppresses notifications from being displayed to the user when a malicious network connection is detected or blocked by the Connector.

### General > Proxy Settings

- **Proxy Host Name** is the name or IP of the proxy server.
- **Proxy Port** is the port the proxy server runs on.
- **Proxy Type** is the type of proxy you are connecting to. The Connector will support *http_proxy*, *socks4*, *socks4a*, *socks5*, and *socks5_hostname*.
- **Proxy Authentication** is the type of authentication used by your proxy server. **Basic** and **NTLM** authentication are supported.
Proxy User Name is used for authenticated proxies. This is the user name you use to connect.

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

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

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

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

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

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

**General > Connector Identity Persistence**

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

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

**None** - Connector logs are not synchronized with new Connector installs under any circumstance.

**By MAC Address across Business** - New Connectors look for the most recent Connector that has the same MAC address to synchronize with across all policies in the business that have Identity Synchronization set to a value other than None.

**By MAC Address across Policy** - New Connectors look for the most recent Connector that has the same MAC address to synchronize with within the same policy.

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

**By Hostname across Policy** - New Connectors look for the most recent Connector that has the same hostname to synchronize with within the same policy.

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

### File Tab

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

#### File > Engines

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

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

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

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

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

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

Monitor Process Execution is the ability for the FireAMP 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 as Passive.

Maximum Scan File Size limits the size of files that are scanned by the FireAMP 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 FireAMP Connector. Any archive file larger than the threshold set will not be scanned.
**File > ETHOS**

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

**File > Scheduled Scans**

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

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

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

When you click **Schedule** an overlay will come up to allow you to choose the **Scan Interval**, **Scan Time**, and **Scan Type**.

**Scan Interval** is how often it should run. The options are **Weekly** or **Monthly**.

**Scan Time** is the time of day you want to kick off the scan.

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

### File > Cloud Policy

**Cloud Policy**

- **Detection Threshold per ETHOS Hash**: 10
- **Detection Threshold per SPERO Hash**: 10
- **Step-Up Enabled**: 
- **Step-Up Threshold**: 5

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

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

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

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

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

### File > Cache Settings

**Cache Settings**

- **Malicious Cache TTL**: 3600
- **Clean Cache TTL**: 604800
- **Unknown Cache TTL**: 3600
- **Application Blocking TTL**: 3600

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

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

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

**Unknown Cache TTL** is the time in seconds that 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 one hour.

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

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

---

**File > Offline Engine - TETRA**

TETRA allows us to perform 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 draw back is compatibility with other antivirus products and should never be enabled if another antivirus product is installed on the computer. This policy configuration option is only available when TETRA has been selected as the Offline Engine under Engines.

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

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

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

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

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

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

Network Tab

The Network tab contains settings for the network flow capabilities of your FireAMP Connectors such as Device Flow Correlation settings.

Network > Device Flow Correlation (DFC)

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

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

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

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

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

**FireAMP Mac Connector**

This section describes the Policy options that are available for FireAMP Mac Connectors. The options are divided into three tabs - General, File, and Network.

**General Tab**

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

**General > Administrative Features**

![Administrative Features]

The **Heartbeat Interval** is the interval in which the Connector calls home to see if there are any files to restore via Cloud Recall™ 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.

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

**General > Client User Interface**

![Client User Interface]

**Start Client User Interface**

**Cloud Notifications**

**Hide File Notifications**

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

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

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

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

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

General > Proxy Settings

Proxy Host Name is the name or IP of the proxy server.
Proxy Port is the port the proxy server runs on.
Proxy Type is the type of proxy you are connecting to. The Connector supports http_proxy.
Proxy Authentication is the type of authentication used by your proxy server. Basic authentication is 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 User Name.

Use Proxy Server for DNS Resolution lets you specify whether all Connector DNS queries should be performed on the proxy server.
Cloud Communication Port allows you to select whether your Connectors perform cloud lookups on TCP 32137 or 443.

General > Product Updates

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

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

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

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

File Tab

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

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

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

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

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

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

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

File > Cache Settings

Malicious Cache TTL 3600
Clean Cache TTL 604800
Unknown Cache TTL 3600
Application Blocking TTL 3600
SHA-256 values are cached to reduce cloud lookup traffic. The amount of time a value is cached depends on the disposition of the file the last time a cloud lookup was performed on its SHA-256. While a file is cached the Connector will always consider its disposition to be what it was the last time a cloud lookup was performed. For example, if a SHA-256 is in an application blocking list and the TTL is 3600 seconds that application will continue to be blocked from execution by the Connector for the next hour even if the administrator removes it from the application blocking list.

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

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

**Unknown Cache TTL** is the time in seconds that 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 one hour.

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

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

---

**File > Engines**

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

**File > Scheduled Scans**

Scheduled scans are not necessary for the operation of the FireAMP Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Cloud Recall™. This allows companies to reduce their energy footprint by eliminating the need for scheduled scans. However, some companies may require scheduled scans due to policy so this can be enabled via policy when necessary.
When you click **Schedule** an overlay will come up to allow you to choose the Scan Interval, Scan Time, and Scan Type.

**Scan Interval** is how often it should run. The options are **Daily**, **Weekly**, or **Monthly**. **Scan Time** is the time of day you want to kick off the scan. **Scan Type** is the type of scan. A **Flash** scan will scan the processes running and the files and registry entries used by those processes. A **Full** scan will scan the processes running, the registry entries, and all the files on disk. This scan is very resource-intensive and should not be performed on a regular basis. A **Custom** scan will scan a particular path that you give it.

**File > Offline Engine - ClamAV**

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

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

**Network Tab**

The Network tab contains settings to for the network flow capabilities of your FireAMP Connectors such as Device Flow Correlation settings.
Enable DFC will enable Device Flow Correlation on your FireAMP Connector. This allows you to monitor network activity and determine which action the Connector should take when connections to malicious hosts are detected.

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

FireAMP Linux Policy

This section describes the Policy options that are available for FireAMP Linux Connectors. The options are divided into three tabs - General, File, and Network.

General Tab

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

General > Administrative Features

The Heartbeat Interval is the interval in which the Connector calls home to see if there are any files to restore via Cloud Recall™ 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.

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

General > Client User Interface

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

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

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

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

**Proxy Type** is the type of proxy you are connecting to. The Connector will support **HTTP_proxy**.

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

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

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

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

General > Product Updates

When a product update is available, you can choose whether or not to update your endpoints on a per-policy basis. You will see an entry in the **Product Version** showing which version you are going to and it will populate the **Update Server** so you can see where the files will be pulled from. You can then configure the **Start Update Window** and **End Update Window**.
The **Update Interval** allows you to specify how long your Connectors will wait between checks for new product updates. This can be configured between every 30 minutes to every 24 hours to reduce network traffic.

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

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

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

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

**File Tab**

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

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

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

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

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

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

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

File > Cache Settings

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

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

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

**Unknown Cache TTL** is the time in seconds that 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 one hour.

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

---

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

---

**File > Engines**

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

---

**File > Scheduled Scans**

Scheduled scans are not necessary for the operation of the FireAMP Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Cloud Recall™. This allows companies to reduce their energy footprint by eliminating the need for scheduled scans. However, some companies may require scheduled scans due to policy so this can be enabled via policy when necessary.
When you click the edit icon an overlay will come up to allow you to choose the Scan Interval, Scan Time, and Scan Type.

**Scan Interval** is how often it should run. The options are **Daily**, **Weekly**, or **Monthly**. **Scan Time** is the time of day you want to kick off the scan. **Scan Type** is 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 only scan files on the path you provide.

**File > Offline Engine - ClamAV**

As a full antivirus product, ClamAV allows us to perform offline scanning. It is signature-based and will take up more disk space on the local computers. By default it will check for updated signatures every 24 hours and download them if new signatures are available. Its major drawback is compatibility with other antivirus products and should never be enabled if another antivirus product is installed on the computer. This policy configuration option is only available when ClamAV has been selected as the Offline Engine under Engines. **Content Update Interval** lets you specify how often your Connectors should check for new ClamAV content such as signatures. Longer update intervals will help to reduce network traffic caused by ClamAV updates while shorter update intervals can consume significant bandwidth and is not recommended for large deployments.

**Network Tab**

The Network tab contains settings for the network flow capabilities of your FireAMP Connectors such as Device Flow Correlation settings.

**Network > Device Flow Correlation (DFC)**

**Enable DFC** will enable Device Flow Correlation on your FireAMP Connector. This allows you to monitor network activity and log any malicious activity.
**Detection Action** can only be set to Audit in order to log activity but not block it.

**Policy Summary**

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

You can also download the XML file that contains the specific policy for the FireAMP Connector using the **Download Policy XML File** button. The FireAMP Connector installer contains the policy by default and this should only be used in specific troubleshooting scenarios.
Groups allow the computers in an organization to be managed according to their function, location, or other criteria determined by the administrator. Click **Create Group** to create a new group. You can also Edit or Delete existing groups. Use **View All Changes** to see a filtered view of the **Audit Log** showing 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.
Groups
Configuring the Group

Chapter 7

Name and Description

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

Parent Menu

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

Policy Menu

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

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

Child Groups

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

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

Adding and Moving Computers

To assign computers to the new group, click Save then go to Management > Computers to add or move computers. See Computer Management for details.
After you have created Policies and assigned them to Groups you can begin deploying the FireAMP Connector to computers and devices in your organization.

Download Connector

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

FireAMP Windows Connector

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

By default you will download a small (~500 KB) bootstrapper file to install the FireAMP Connector. This executable determines if the computer is running a 32- or 64-bit operating system and downloads and installs the appropriate version of the FireAMP Connector. You can also choose to download a redistributable installer. This is a 30 MB file that contains both the 32- and 64-bit installers. This file can be placed on a network share or pushed to all the computers in a group via a tool like System Center Configuration Manager in order to install the FireAMP Connector on multiple computers. The bootstrapper and redistributable installer also both contain 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 FireAMP 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.

**FireAMP Mac Connector**

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

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

**FireAMP Linux Connector**

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

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

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

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

The Deployment Summary page gives you a list of the successful and failed FireAMP 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 FireAMP Connector version. In some cases the install failed completely and a reason will be given, 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 FireAMP Connector to endpoints they will begin to appear on the Computers screen accessible from Management > Computers. The computer list shows all the endpoints that have installed the FireAMP Connector. View All Changes will take you to a filtered view of the Audit Log showing 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 all computers or certain computers in order to move them to another group, a new group, or to delete them. Select one or more computers and click Export to CSV to download a list of computers including Connector GUID, Hostname, Operating System, Connector Version, Group, Connector Install Date, and the Last Seen date.

IMPORTANT! All dates and times in the exported CSV file will be in UTC regardless of your Time Zone Settings.
Clicking on a computer in the list will expand details on that computer. Clicking the + or - buttons will expand or collapse the details for every computer on the current page. From the detail you can change the Groups the computer belongs to, see which Policies applies to it, along with other information about the computer. 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 showing all changes for the specific computer.

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

If you click Scan a dialog will be displayed allowing 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 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.

You can also click the Browse events for this computer button to open a filtered Events Tab view for the selected computer.
CHAPTER 9

FIREAMP WINDOWS CONNECTOR

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

System Requirements

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

**Microsoft Windows 7**
- 1 GHz or faster processor
- 1 GB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

**Microsoft Windows 8 and 8.1 (requires FireAMP Windows Connector 3.1.4 or later)**
- 1 GHz or faster processor
- 512 MB RAM
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA

**Microsoft Windows 10 (requires FireAMP Windows Connector 4.3.0 or later)**
- 1 GHz or faster processor
- 1 GB RAM (32-bit) or 2 GB RAM (64-bit)
- 650 MB available hard disk space - Cloud-only mode
- 1 GB available hard disk space - TETRA
Microsoft Windows Server 2008 R2
- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space – Cloud only mode
- 1 GB available hard disk space – TETRA

Microsoft Windows Server 2012 and 2012 R2 (requires FireAMP Windows Connector 3.1.9 or later)
- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space – Cloud only mode
- 1 GB available hard disk space – TETRA

Microsoft Windows Server 2016 (requires FireAMP Windows Connector 6.0.9 or later)
- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space – Cloud only mode
- 1 GB available hard disk space – TETRA

Previously Supported Versions

Microsoft Windows XP with Service Pack 3 or later (requires FireAMP Windows Connector versions 5.x.x or lower)
- 500 MHz or faster processor
- 256 MB RAM
- 650 MB available hard disk space – Cloud-only mode
- 1 GB available hard disk space – TETRA

Microsoft Windows Vista with Service Pack 2 or later (requires FireAMP Windows Connector versions 5.x.x or lower)
- 1 GHz or faster processor
- 512 MB RAM
- 650 MB available hard disk space – Cloud-only mode
- 1 GB available hard disk space – TETRA

Microsoft Windows Server 2003 (requires FireAMP Windows Connector versions 5.x.x or lower)
- 1 GHz or faster processor
- 512 MB RAM
- 650 MB available hard disk space – Cloud-only mode
- 1 GB available hard disk space – TETRA

Microsoft Windows Server 2008 (requires FireAMP Windows Connector versions 5.x.x or lower)
- 2 GHz or faster processor
- 2 GB RAM
- 650 MB available hard disk space – Cloud only mode
- 1 GB available hard disk space – TETRA
Incompatible software and configurations

The FireAMP Windows Connector is currently not compatible with the following software:

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

The FireAMP Windows Connector does not currently support the following proxy configurations:

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

Firewall Connectivity

To allow the FireAMP Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are two sets of servers depending on where you are located - one for the European Union and one for the rest of the world.

**IMPORTANT!** If your firewall requires IP address exceptions see the Cloud Connection Tool accessible from Management > Policies in the FireAMP Console.

Firewall Exceptions

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

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.immunet.com
- **Endpoint IOC Downloads** - ioc.amp.cisco.com
- **Advanced Custom Signatures** - custom-signatures.amp.cisco.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - console.amp.cisco.com
To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443:

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

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

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

### European Union Firewall Exceptions

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

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

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

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

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

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

### Proxy Autodetection

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

The FireAMP Connector can be set to discover endpoint proxy settings automatically. Once the Connector detects proxy setting information it attempts to connect to the FireAMP Management Server to confirm 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 FireAMP Management Server it will attempt to retrieve proxy settings from the Windows registry on the endpoint. The Connector will attempt to retrieve the settings only from system-wide settings and not per-user settings.

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

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

Installer

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

Interactive Installer

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

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

![User Account Control](https://example.com/user-account-control.png)
At this point the Download Manager will fetch the appropriate version of the installer package if installing through the bootstrapper. If the redistributable installer is used then this step will be skipped.

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

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

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

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

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

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

**IMPORTANT!** This must be specified as the first parameter.

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

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

- /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.

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

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

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

Connector User Interface

When the Connector is installed you can access it by double-clicking the desktop shortcut or clicking the FireAMP Connector entry in the Windows Start Menu.

From the FireAMP Connector main screen you can choose to launch a scan, view the Connector history, or view the Connector settings. The Connector status is also shown indicating whether it is connected to the network or if the service is stopped, when the last scan was performed, and the policy currently applied to the Connector. These entries can be useful in diagnosing Connector issues.
Scanning

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

Available scanning options are:

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

**Custom Scan** - Allows the user to define specific files or directories to scan. Selecting the 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 (ie. USB drives). This scan can be time-consuming and resource-intensive so should only be performed once when the Connector is first installed.

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

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

There are different views available in the History:

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

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

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

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

Settings

The Settings interface allows the individual user to see how the policy administrator has chosen to configure all aspects of the policy applied to the particular Connector. In a managed install all the entries in the settings are read-only and provided solely for informational and diagnostic purposes.
The Sync Policy button allows you to check for a policy update outside of the normal heartbeat interval. This is particularly useful during an outbreak situation where new custom detections have been added or if programs have been added or removed from whitelists and application blocking lists.

Uninstall

To uninstall a Connector from an endpoint, select Control Panel from the Start Menu. Under Programs select Uninstall a program. Select FireAMP Connector in the program list then click Uninstall/Change. Click the Uninstall button on the dialog box to remove
the application. If a password requirement to uninstall the Connector has been set in Policy you will be prompted to enter it.

![Password Required]

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 FireAMP Connector history and quarantine files. Reboot the computer to complete the uninstall process.

**IMPORTANT!** On Windows 8 and higher if Fast Startup mode is enabled you should reboot the computer after uninstall is complete rather than using the Windows Shut down option. This will ensure that the final cleanup steps to remove the Connector drivers complete properly.
CHAPTER 10
FIREAMP MAC CONNECTOR

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

System Requirements

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

**Apple OS X 10.11 (requires FireAMP Mac Connector 1.0.7 or later)**
- 2 GB RAM
- 1.5 GB available hard disk space

**Apple OS X 10.12 (requires FireAMP Mac Connector 1.2.4 or later)**
- 2 GB RAM
- 1.5 GB available hard disk space

**Apple macOS 10.13 (requires FireAMP Mac Connector 1.5.0 or later)**
- 2 GB RAM
- 1.5 GB available hard disk space

Previously Supported Versions

**Apple OS X 10.7 (requires FireAMP Mac Connector 1.2.6 or earlier)**
- 2 GB RAM
- 65 MB available hard disk space
Incompatible Software and Configurations

The FireAMP Mac Connector does not currently support the following proxy configurations:

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

Firewall Connectivity

To allow the FireAMP Connector to communicate with Cisco systems, the firewall must allow the clients to connect to certain servers over specific ports. There are two sets of servers depending on where you are located - one for the European Union and one for the rest of the world.

**IMPORTANT!** If your firewall requires IP address exceptions see the Cloud Connection Tool accessible from Management > Policies in the FireAMP Console.

Firewall Exceptions

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

- **Event Server** - intake.amp.cisco.com
- **Management Server** - mgmt.amp.cisco.com
- **Policy Server** - policy.amp.cisco.com
- **Error Reporting** - crash.immunet.com
- **Connector Upgrades** - upgrades.amp.cisco.com
- **Remote File Fetch** - console.amp.cisco.com
To allow the Connector to communicate with Cisco cloud servers for file and network disposition lookups the firewall must allow the clients to connect to the following server over TCP 443 by default or TCP 32137:

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

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

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

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

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

### European Union Firewall Exceptions

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

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

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

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

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

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

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

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

### Installing the FireAMP Mac Connector

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

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

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

Using the FireAMP Mac Connector

The FireAMP Mac Connector user interface is a menulet that appears on your Mac’s menu bar.

The menulet primarily provides information such as when the last scan was performed, the current status, and the policy the Connector is using. You can also start, pause, and cancel scans from the menulet.
Sync Policy will check to make sure your Connector is running the most recent version of the policy. If not, it will download the latest version.

Versions 1.2 and higher of the FireAMP Mac Connector use a command line interface in addition to a graphical user interface on endpoints. The FireAMP Mac Connector command line interface can be found at /usr/local/libexec/sourcefire/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.

Settings

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

Mail.app

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

Uninstall

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

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

1. /bin/launchctl unload /Library/LaunchAgents/com.sourcefire.amp.agent.plist
   If this does not stop the menulet, click on it and select Quit FireAMP Connector.
2. sudo /bin/launchctl unload /Library/LaunchDaemons/com.sourcefire.amp.daemon.plist
3. sudo /bin/launchctl list com.sourcefire.amp.daemon
   This should yield an empty list.
4. sudo /sbin/kextunload -b com.sourcefire.amp.fileop
5. sudo /sbin/kextunload -b com.sourcefire.amp.nke
6. sudo /usr/sbin/kextstat -l | grep com.sourcefire
   This should yield an empty list.
7. sudo rm -rf /Applications/FireAMP
8. `sudo rm -rf /Library/Extensions/ampfileop.kext`
9. `sudo rm -rf /Library/Extensions/ampnetflow.kext`
10. `sudo rm -rf /Library/Application\Support/Sourcefire/FireAMP\Mac`
11. `sudo rm -rf /usr/local/libexec/sourcefire`
12. `sudo pkgutil --forget com.sourcefire.amp.agent`
13. `sudo pkgutil --forget com.sourcefire.amp.kextsigned`
14. `sudo pkgutil --forget com.sourcefire.amp.kextunsigned`
15. `sudo pkgutil --forget com.sourcefire.amp.support`
16. `sudo pkgutil --forget com.sourcefire.amp.daemon`
After you have defined groups, policies, and a deployment strategy, the FireAMP Connector can be installed on the endpoints. This section will go through the manual install process and highlight some of the key features of the Connector user interface.

System Requirements

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

**RHEL/CentOS 6.8 (requires FireAMP Linux Connector 1.5.1 or later)**
- 2 GB RAM
- 1.5 GB available hard disk space

**RHEL/CentOS 6.9 (requires FireAMP Linux Connector 1.5.1 or later)**
- 2 GB RAM
- 1.5 GB available hard disk space

**RHEL/CentOS 7.3 (requires FireAMP Linux Connector 1.5.1 or later)**
- 1 GB RAM
- 1.5 GB available hard disk space

**RHEL/CentOS 7.4 (requires FireAMP Linux Connector 1.5.1 or later)**
- 2 GB RAM
- 1.5 GB available hard disk space

**IMPORTANT!** The FireAMP Linux Connector may not install properly on custom kernels. If you have a custom kernel, contact Support before attempting to install.
Previously Supported Versions

**RHEL/CentOS 6.5/6.6/6.7 (requires FireAMP Linux Connector 1.6.0 or earlier)**
- 1 GB RAM
- 400 MB available hard disk space

**RHEL/CentOS 7.2 (requires FireAMP Linux Connector 1.6.0 or earlier)**
- 1 GB RAM
- 400 MB available hard disk space

Incompatible software and configurations

The FireAMP Linux Connector is currently not compatible with the following software:
- F-Secure Linux Security
- Kaspersky Endpoint Security
- McAfee VSE for Linux
- Sophos Server Security 9
- Symantec Endpoint Protection
- Tripwire

The FireAMP Linux Connector does not currently support the following proxy configurations:
- SOCKS proxies.
- HTTP proxies with NTLM authentication.

The FireAMP Linux Connector may cause unmount failures with removable media or temporary file systems mounted in non-standard locations. 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.

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

Firewall Connectivity

To allow the FireAMP Connector to communicate with Cisco cloud servers, the firewall must allow the clients to connect to certain servers over specific ports. There are two sets of servers depending on where you are located – one for the European Union and one for the rest of the world.

**IMPORTANT!** If your firewall requires IP address exceptions see the Cloud Connection Tool accessible from Management > Policies in the FireAMP Console.
FireAMP Linux Connector
Installing the FireAMP Linux Connector

Chapter 11

Firewall Exceptions

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

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

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

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

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

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

European Union Firewall Exceptions

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

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

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

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

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

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

Installing the FireAMP Linux Connector

To install the Connector execute the following command:

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

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

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

To import the GPG key:

1. Verify the GPG key by clicking the GPG Public Key link on the Download Connector page. Compare the key to the one at /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp.
2. Run the following command from a terminal to import the key: sudo rpm --import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp
3. Verify the key was installed by running the following command from a terminal: rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
4. Look for a GPG key from Sourcefire in the output.

Using the FireAMP Linux Connector

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

Support Tool

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

   sudo ./ampsupport

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

   sudo ./ampsupport -o [path]

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

Uninstall

To uninstall the FireAMP Linux Connector, execute the following command:

   sudo yum remove ciscoampconnector -y

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

   /opt/cisco/amp/bin/purge_amp_local_data
CHAPTER 12
ENDPOINT IOC SCANNER

The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers. Endpoint IOCs are imported through the console from OpenIOC-based files written to trigger on file properties such as name, size, hash, and other attributes and system properties such as process information, running services, and Windows Registry entries. The IOC syntax can be used by incident responders to find specific artifacts or 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 FireAMP 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 currently supported by the IOC Scanner and links to sample Endpoint IOC documents see the Cisco Endpoint IOC Attributes guide.

Installed Endpoint IOCs

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

Uploading Endpoint IOCs

Endpoint IOCs have to be uploaded to the FireAMP Console before you can initiate scans. When you navigate to the Installed Endpoint IOCs page use the Upload button
to transfer your Endpoint IOCs. You can upload a single XML file or a zip archive containing multiple Endpoint IOC documents.

**IMPORTANT!** There is a 5 MB file upload limit.

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

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

**View and Edit**

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

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

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

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

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

**Activate Endpoint IOCs**

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

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

**Initiate Scan**

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

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

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

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

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

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

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

Both the **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

The **Full Scan** adds the following:

- The entire Windows registry using the hives on disk
- All files and directories on the file system
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 FireAMP Connector 4.4 and higher), or run the scan without cataloging. A full catalog will take the most time to complete and running the scan without a catalog will take the least amount of time. If you choose to only catalog changes then only changes to the filesystem since the last full catalog will be cataloged. The amount of time this scan takes will vary based on the number of changes to catalog.

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

Scan by Computer

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

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

When you click Start Scan the FireAMP 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 FireAMP 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 showing 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 FireAMP Dashboard.
Search allows you to find various information from your FireAMP 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 FireAMP 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 the 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 FireAMP 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
- FireAMP Policy names
- FireAMP Group names
- device names (prefix match only)

Searches by exact file extension like ‘.exe’ and ‘.pdf’ can also be performed to find all files observed with those extensions.
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 by exact host name or a sub-domain. These searches will return any files that your FireAMP Connectors downloaded from those hosts and any FireAMP Connectors that contacted that host.
CHAPTER 14
FILE ANALYSIS

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

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

File Analysis Landing Page

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

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

If the file you are looking for has not been analyzed already, you can choose to upload the file (up to 20MB) to be analyzed. To do this, click Submit File, select the file you want to upload using the Browse button, select the virtual machine operating system image to run it in, then click the Upload button. After the file has been uploaded it
takes approximately 30 to 60 minutes for the analysis to be available, depending on system load.

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

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

The File Analysis sandbox has the following limitations:

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

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

**Threat Analysis**

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

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

When analyzing malware a video of the execution is also captured. The video can be used to observe the visual impact that the malware has on the desktop of a victim. The video can be used in user education campaigns, 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.

**Analysis Report**

- **ID**: 31a15d41803231d645cbe1978553085
- **OS**: 2600.wpsp 090413-2111
- **Started**: 12/26/14 18:08:00
- **Ended**: 12/26/14 18:14:14
- **Duration**: 0:06:14
- **Sandbox**: cubonia (pilot-d)
- **Filename**: 0b3f4dc42e8d31e51739e09e56003b9546b094f1f151daecf8aba4ac5c074b8.exe
- **Magic Type**: PE32 executable (GUI) Intel 80386, for MS Windows
- **Analyzed As**: exe
- **SHA256**: 0b3f4dc42e8d31e51739e09e56003b9546b094f1f151daecf8aba4ac5c074b8
- **SHA1**: 4d70e1189496e6c617f36b8382b7b6875ed549
- **MD5**: e09d1e45c5d97128e6d8e2a71c218ad

**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 AMP Threat Grid analysis.

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

**SHA256** - The SHA-256 cryptographic hash function output.

**SHA1** - The SHA1 cryptographic hash function output.

**MD5** - The MD5 cryptographic hash function output.

**Warnings** - High level descriptions of potentially harmful activities.

**Behavioral Indicators**

The analysis report provides a summary of the Behavioral Indicators generated by AMP Threat Grid analysis. These Behavioral Indicators quickly explain any behaviors that
might indicate malicious or suspicious activity. AMP Threat Grid generates Behavioral Indicators during analysis, after the analysis of the malware activities is complete.

**Behavioral Indicators**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Severity</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Created an Executable in a System Directory</td>
<td>100</td>
<td>90</td>
</tr>
<tr>
<td>Adware Hotbar Detected</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified an Executable File</td>
<td>85</td>
<td>95</td>
</tr>
<tr>
<td>Process Modified a File in a System Directory</td>
<td>80</td>
<td>100</td>
</tr>
<tr>
<td>Downloaded PE Executable</td>
<td>80</td>
<td>95</td>
</tr>
<tr>
<td>Process Created a File in the Windows Startup Folder</td>
<td>60</td>
<td>50</td>
</tr>
<tr>
<td>Outbound HTTP GET Request</td>
<td>75</td>
<td>75</td>
</tr>
<tr>
<td>Process Modified File in a User Directory</td>
<td>70</td>
<td>80</td>
</tr>
<tr>
<td>Process Disabled Internet Explorer Proxy</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>Potential Code Injection Detected</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

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.

**Behavioral Indicators**

- **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** - Name of the antivirus product that flagged the sample as potentially malicious.
- **Antivirus Result** - Results of the flagged antivirus product.
- **Artifact ID** - 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.

<table>
<thead>
<tr>
<th>Path</th>
<th>Process Name</th>
<th>Process ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\yhtzcent-2.exe</td>
<td>2203v5-1000-88888.exe</td>
<td>1804 [2203v5-1000-88888.exe]</td>
</tr>
</tbody>
</table>
HTTP Traffic

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

**HTTP Traffic**

<table>
<thead>
<tr>
<th>HTTP Command</th>
<th>Server IP</th>
<th>Server Port</th>
<th>Resp. Content</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET <a href="http://url2bkan.com:80/url.asp">http://url2bkan.com:80/url.asp</a></td>
<td>123.57.37.211</td>
<td>80</td>
<td>text/plain</td>
<td>+102.81s</td>
</tr>
<tr>
<td>GET <a href="http://url2bkan.com:80/ip.asp">http://url2bkan.com:80/ip.asp</a></td>
<td>123.57.37.211</td>
<td>80</td>
<td>text/plain</td>
<td>+114.158s</td>
</tr>
<tr>
<td>GET <a href="http://softlj.srvpj.com:80/ij.php?ip=66.187.149.88&amp;mac=00-50-E5-45-56-87&amp;sd=4l...C4C1E6B5F">http://softlj.srvpj.com:80/ij.php?ip=66.187.149.88&amp;mac=00-50-E5-45-56-87&amp;sd=4l...C4C1E6B5F</a></td>
<td>182.92.185.161</td>
<td>80</td>
<td>text/plain</td>
<td>+117.223s</td>
</tr>
<tr>
<td>GET <a href="http://url0755look.com:30/tj.asp?uid=">http://url0755look.com:30/tj.asp?uid=</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DNS Traffic

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

**DNS Traffic**

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Query Data</th>
<th>TTL</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>update.yoyolm.net</td>
<td>3127</td>
<td>+267.541s</td>
</tr>
<tr>
<td>A</td>
<td>dj360safe.com</td>
<td>-</td>
<td>+285.479s</td>
</tr>
<tr>
<td>A</td>
<td>url2bkan.com</td>
<td>-</td>
<td>+102.241s</td>
</tr>
<tr>
<td>A</td>
<td>softlj.srvpj.com</td>
<td>-</td>
<td>+116.894s</td>
</tr>
<tr>
<td>A</td>
<td><a href="http://www.baidu.com">www.baidu.com</a></td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

TCP/IP Streams

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

Move the cursor over the Src. IP address to display a pop-up listing all the Source Network IP addresses of the network stream that have been detected by AMP Threat Grid during analysis.
Clicking on one of the network streams will open a web page with the appropriate network stream.

**TCP/IP Streams**

<table>
<thead>
<tr>
<th>Network Stream: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src. IP: 172.16.1.1</td>
</tr>
<tr>
<td>Artifacts: 0</td>
</tr>
<tr>
<td>Src. Port: 2</td>
</tr>
<tr>
<td>Packets: 2</td>
</tr>
<tr>
<td>Bytes: 56</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Stream: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src. IP: 172.16.10.247</td>
</tr>
<tr>
<td>Artifacts: 0</td>
</tr>
<tr>
<td>Src. Port: 2</td>
</tr>
<tr>
<td>Packets: 2</td>
</tr>
<tr>
<td>Bytes: 80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Stream: 2 (DNS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src. IP: 172.16.10.247</td>
</tr>
<tr>
<td>Artifacts: 0</td>
</tr>
<tr>
<td>Src. Port: 1031</td>
</tr>
<tr>
<td>Packets: 65</td>
</tr>
<tr>
<td>Bytes: 9591</td>
</tr>
</tbody>
</table>

**Processes**

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

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Name</th>
<th>Actions</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Details]</td>
<td>1000</td>
<td>tqli_158_1.exe</td>
<td>File Actions: 3</td>
<td>Analysis Reason: Parent is being analyzed.</td>
</tr>
<tr>
<td>[Details]</td>
<td>1132</td>
<td>BaiduBrowserOnlineSetupSilent-537-ftr_300000062.exe</td>
<td>File Actions: 3</td>
<td>Analysis Reason: Parent is being analyzed.</td>
</tr>
<tr>
<td>[Details]</td>
<td>1152</td>
<td>hituid_36575.exe</td>
<td>File Actions: 3</td>
<td>Analysis Reason: Parent is being analyzed.</td>
</tr>
<tr>
<td>[Details]</td>
<td>1364</td>
<td>hituid_70673.exe</td>
<td>File Actions: 3</td>
<td>Analysis Reason: Parent is being analyzed.</td>
</tr>
</tbody>
</table>

**Artifacts**

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

<table>
<thead>
<tr>
<th>Artifact</th>
<th>Created</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Details]</td>
<td>1804</td>
<td>Documents and Settings\Administrator\r4.0008828699(1).txt</td>
</tr>
<tr>
<td>[Details]</td>
<td>780</td>
<td>Documents and Settings\Admin\TTKdump.dll</td>
</tr>
</tbody>
</table>
Registry Activity

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

### Registry Activity

- Created Keys
- Modified Keys
- Deleted Key Values

Filesystem Activity

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

### Filesystem Activity

<table>
<thead>
<tr>
<th>Path</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:</td>
<td>Documents and Settings</td>
</tr>
<tr>
<td>C:</td>
<td>Documents and Settings</td>
</tr>
<tr>
<td>C:</td>
<td>Documents and Settings</td>
</tr>
<tr>
<td>C:</td>
<td>Documents and Settings</td>
</tr>
<tr>
<td>C:</td>
<td>Documents and Settings</td>
</tr>
<tr>
<td>C:</td>
<td>Documents and Settings</td>
</tr>
</tbody>
</table>
CHAPTER 15
TRAJECTORY

Trajectory shows you activity within your FireAMP deployment, either across multiple computers or on a single computer. When you navigate to the Trajectory page the three most recent files and devices observed in your environment are displayed.

File Trajectory

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

Description

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

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

File Trajectory displays the following file types:

- Executable files
- Portable Document Format (PDF) files
- MS Cabinet files
- MS Office files
• Archive files
• Adobe Shockwave Flash
• Plain text files
• Rich text files
• Script files
• Installer files

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

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

Created By – identifies the files that created the threat in question by their SHA-256. This includes the number of times the threat was created by that file in both your network and among all FireAMP 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** - Expand this section to show additional information about the file in question.

- **Known As** shows the SHA-256, SHA-1, and MD5 hash of the file.
- **Attributes** displays the file size and type.
- **Known Names** includes any names the file went by on your network.
- **Detected As** shows any detection names in the case of a malicious file.

**IMPORTANT!** For descriptions of threat names, see [AMP Naming Conventions](#).

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

- **Connections Flagged As** shows any activity that corresponds to an IP Black 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:

- 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
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 FireAMP Connector. It tracks file, network, and Connector events such as policy updates in chronological order. This gives you visibility into the events that occurred leading up to and following a compromise, including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware.

**Description**

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

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

Device Trajectory displays the following file types:

- Executable files
- Portable Document Format (PDF) files
- MS Cabinet files
- MS Office files
- Archive files
- Adobe Shockwave Flash
- Plain text files
- Rich text files
- Script files
- Installer files

**IMPORTANT!** A maximum of 4000 objects are rendered in the Device Trajectory view. If you navigate to Device Trajectory from the Computers page you will see the 4000 most recent objects. If you navigate to Device Trajectory from a specific event you will see up to 4000 objects related to that event.

The vertical axis of the Device Trajectory shows a list of files and processes observed on the computer by the FireAMP Connector and the horizontal axis represents the time and date. Running processes are represented by a solid horizontal line with child
processes and files the process acted upon stemming from the line. Click on an event to view its details.

File events include the file name, path, parent process, file size, execution context, and hashes for the file. For malicious files, the detection name, engine that detected the file, and the quarantine action are also shown.

**IMPORTANT!** For descriptions of threat names, see [AMP Naming Conventions](#).

Network events include the process attempting the connection, destination IP address, source and destination ports, protocol, execution context, file size and age, the process ID and SID, and the file’s hashes. For connections to malicious sites, the detection name and action taken will also be displayed.

FireAMP Connector events are displayed next to the [System] label in Device Trajectory. Connector events include reboots, user-initiated scans and scheduled scans, policy and definition updates, Connector updates, and a Connector uninstall.

You can use the slider below the device trajectory to narrow the scope of the trajectory to a specific time and date range. The left handle of the slider changes the beginning of the trajectory view and the right handle limits the end of the view. This can help you see the trajectory of events in a particular time range with greater clarity.

**Indications of Compromise**

When certain series of events are observed on a single computer, they are seen by FireAMP as Indications of Compromise. In Device Trajectory these events will be highlighted yellow so they are readily visible. There will also be a separate compromised event in the Trajectory that describes the type of compromise. Clicking
on the compromised event will also highlight the individual events that triggered it with a blue halo.

For Indication of Compromise descriptions, please see Threat Descriptions.

Filters and Search

Device Trajectory can contain a large amount of data for computers that see heavy use. To narrow Device Trajectory results for a computer, you can apply filters to the data or search for specific files, IP addresses, or threats. You can also use filters in combination with a search to obtain even more granular results.

Filters

There are four event filter categories in Device Trajectory – Event Type, Event Disposition, Event Flags, and File Type. You must select at least one item from each category to view results.

**Event Type** are events that the FireAMP Connector recorded. File, network, and Connector activity are represented. File events can include a copy, move, execution, and other operations. Network events include both inbound and outbound connections to both local and remote addresses. Connector activity can include reboots, policy updates, scans, and uninstalls.

**Event Disposition** allows you to filter events based on their disposition. You can choose to view only events that were performed on or by malicious files, clean files, or those with an unknown disposition.

**Event Flags** are modifiers to event types. For example, a warning may be attached to a malicious file copy event because the malicious file was detected but not successfully quarantined. Other events such as a scan that did not complete successfully or a failed policy update may also have a warning flag attached.

The audit only flag means that the events in question were observed but not acted upon in any way because the **File Conviction Mode** policy item under File > Modes or the **Detection Action** policy item under Network > Device Flow Correlation (DFC) was set to **Audit**.

**File Type** allows you to filter Device Trajectory events by the type of files involved. You can filter by the file types most commonly implicated in malware infections such as executables and PDFs. The **other** filter is for all file types not specifically listed, while the **unknown** filter is for files that the type was undetermined possibly due to malformed header information.
Search

The search field on the Device Trajectory page allows you to narrow the Device Trajectory to only show specific results. Searches can be simple text strings, a regular expression supported by JavaScript in the /foo/gim format where the gim are optional flags, or a CIDR address in the format X.X.X.X/Y. You can also drag and drop a file into the search box on browsers that support this, which will calculate the SHA-256 value of the file and insert the string in the search box.

Within Device Trajectory events there are several terms you can search by including:

- Detection name
- SHA-256
- SHA-1
- MD5
- File name
- Directory name
- Local and remote IP addresses
- Port numbers
- URLs
The File Repository allows you to download files you have requested from your FireAMP 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.

On Private Cloud devices you can manually request files up to 20MB in size or up to 5MB through Automatic Analysis. The File Repository in Proxy Mode stores up to 500 manually fetched files and up to 160 automatically requested files. In Standalone Modes the appliance stores up to 200,000 requested files. If the limit is reached then the oldest files will be deleted when new files are requested.

**IMPORTANT!** You must have Two-Step Verification enabled on your account to request files from your Connectors and download them from the File Repository. Files can only be fetched from computers running version 3.1.9 or later of the FireAMP Windows Connector, version 1.0.2.6 or later of the FireAMP Mac Connector, and version 1.0.2.261 or later of the FireAMP 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 FireAMP 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 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 FireAMP Connector to download the file from. If the file was observed by more than one Connector you can use the drop
File Repository

Requesting a remote file

Chapter 16

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 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 FireAMP Connector observed it. This can occur if the file was deleted from the computer or 3rd party antivirus software quarantined the file. Files with a clean disposition cannot be retrieved unless they were copied to a different location. In these cases you can attempt to fetch the file from a different computer or manually retrieve the file from quarantine.
Chapter 17
Threat Root Cause

Threat Root Cause helps identify legitimate and rogue applications that are at high risk for introducing malware into your environment. It focuses on software that is observed installing malware onto computers.

Select Dates

Threat Root Cause allows you to select a date range to view. By default the date range is set to show the previous day and current day. Select the start and end dates you want to view then click Reload to view the Threat Root Cause for the specified date range.

Overview

The Threat Root Cause Overview tab shows the top ten software packages by name 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.

<table>
<thead>
<tr>
<th>Program</th>
<th>Threat Name</th>
<th>Version</th>
<th>Threats Introduced</th>
<th>Computers Affected</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>explorer.exe</td>
<td></td>
<td>6.0.2900.5512</td>
<td>44</td>
<td>3</td>
<td>44 moved</td>
</tr>
<tr>
<td>a.exe</td>
<td></td>
<td>12</td>
<td>4 created</td>
<td>4 executed</td>
<td>4 moved</td>
</tr>
<tr>
<td>a.exe</td>
<td></td>
<td>12</td>
<td>4 created</td>
<td>4 executed</td>
<td>4 moved</td>
</tr>
<tr>
<td>iexplore.exe</td>
<td></td>
<td>8.0.6001.18702</td>
<td>10</td>
<td>5</td>
<td>8 created</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>4 created</td>
<td>2 executed</td>
<td></td>
</tr>
<tr>
<td>java.exe</td>
<td></td>
<td>7.0.100.18</td>
<td>5</td>
<td>1</td>
<td>3 created</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>4 created</td>
<td>2 executed</td>
<td></td>
</tr>
<tr>
<td>iexplore.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dwm.exe</td>
<td></td>
<td>6.1.7600.16385</td>
<td>5</td>
<td>1</td>
<td>3 created</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>regsvr32.exe</td>
<td></td>
<td>6.1.7600.16385</td>
<td>3</td>
<td>1</td>
<td>2 created</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
Prevalence displays files that have been executed across your organization ordered from lowest to highest. 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) or questionable applications you may not want in your network.

Low Prevalence Executables

The page shows each file that was executed and which computer it was executed on. 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. 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 executable files from specific groups to File Analysis. Click Configure Automatic Analysis to choose your groups.

**IMPORTANT!** You must have the File Repository enabled 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 Enable.

Once you have configured Automatic Analysis, low prevalence executable files will be submitted every 4 hours. FireAMP will request the file from the FireAMP Connector that observed it if it is available. Once the file has been retrieved it will be submitted to File Analysis. You can then view the results of the analysis from the File Analysis page. If the file is not retrieved for a period of time, you can check the file fetch status in the File Repository.

**IMPORTANT!** There are limits on files that can be sent for automatic analysis through your device. There is a 5MB file size limit and up to 160 files can be stored in the File Repository. Once a file has successfully been sent to your Threat Grid appliance for analysis it is removed from the File Repository and can be viewed or downloaded from Threat Grid instead.
Whenever an executable file is moved, copied, or executed the FireAMP 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:

- Program name and version.
- SHA-256 value for the executable file.
- Number of computers in the defined group that the FireAMP Connector observed the file on.
- Number of severe vulnerabilities known to be present in the executable. See **Common Vulnerabilities and Exposures**.
- CVSS score of the most severe vulnerability in the executable. See **Common Vulnerability Scoring System**.

**Common Vulnerabilities and Exposures**

The Common Vulnerabilities and Exposures (CVE) database records known vulnerabilities in various applications. All vulnerabilities are noted by their unique CVE ID. The CVE ID shown in the console can be clicked to get more details on the vulnerability.

Clicking on the CVE ID link brings you to a page that defines the vulnerability and lists any patches if available.

**Common Vulnerability Scoring System**

The Common Vulnerability Scoring System (CVSS) is designed to allow a user to determine which priority level to assign to an identified vulnerability. The scale goes from 0 (lowest) to 10 (highest).
Clicking on an item in the list of identified vulnerable programs shows the ten most severe and recent vulnerabilities with a CVSS score higher than 5.9.

Additional Information on Vulnerable Software

Additional information is available at the bottom of the expanded program list item. The following topics provide additional information through the associated links:

- **Observed in Groups**
- **Last Observed** (computer)
- **Events**
- **File Trajectory**

Additionally, the **Filename** indicates the file name of the executable file.

**Observed in Groups**

The link (for example, Audit) is the name of the defined group that the computers belong to. For more information see **Groups**.

**Last Observed**

The time and date and on which computer the vulnerability was last observed. The machine name is a link to a page which provides additional details on the computer. For more information see **Computer Management**.

**Events**

Clicking on the **Events** link opens the **Dashboard** and shows the contents of the **Events** tab. For more information, see **Events Tab**.
Vulnerable Software

Chapter 19

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**.
Reports allow you to view aggregate data generated in your business over a one week period. They can be accessed from Analysis > Reports on the main menu.

Creating a Report

Reports cover a one week period beginning every Sunday at midnight until midnight the following Sunday (UTC). Weekly reports are created automatically but you can choose whether to receive the reports via email.

Report Sections

Each report section links to the appropriate section of the FireAMP Console so you can drill down further into the data.

IMPORTANT! The data displayed in the Console may not match the report data exactly if any retrospective jobs were run after the report was generated.

Active Connectors

Shows the number of active Connectors in the business compared to the previous week. To be considered active, a Connector must have checked in at least once in the 7 day period. The number of new installs and uninstalls are also shown.

Infected Computers Comparison

Shows the number of computers that observed both file-based and network-based detections this week compared to the previous week. The top five computers
observing malware are also listed along with the number of malicious file and network detections each saw.

File Detections
Shows the top five computers seeing file detections over the week and the top five files detected. You can also see the daily detection rates for the current week compared to the previous week.

Network Detections
Shows the top five computers seeing network detections over the week and the top five IP addresses detected. You can also see the daily detection rates for the current week compared to the previous week.

Quarantines
Shows the daily successful quarantine rate for the current week compared to the previous week.

Application Blocks
Shows successful application blocks for the week based on your Application Control - Blocking lists.

Retrospective Detections
Shows the number of files seen by your Connectors that had their disposition changed to malicious and were retroactively quarantined.

Retrospective False Positives
Shows the number of files seen by your Connectors initially categorized as malicious that had their disposition changed to clean and were retroactively restored from quarantine.

Indications of Compromise
Shows the number of times Indications of Compromise were triggered for the week.
Items under the Accounts menu allow you to manage your FireAMP console. User management, defaults, and audit logs can all be accessed from this menu.

**Users**

The Users screen allows you to manage accounts and view notifications and subscriptions for that account.

You can search the user list by name or email address. You can also sort the list by email address, name, or last login time. Accounts with a key next to them are administrators and those without are unprivileged users. Click the My Account link to view the account you are currently logged in as. This account will also be highlighted blue in the user list.

Clicking the clock icon next to a user account will allow you to see a filtered view of the Audit Log for activity related to that account. You can also click the View All Changes link to see a filtered view of the Audit Log showing all activity for user accounts.

When you select an account by clicking on the Name or Email Address you can see different options for it including options to edit the account. If you select your own account you also have the option to reset your password.

Click on New User to create a new FireAMP console user account. A valid email address is required for them to receive an account activation email. You can also add a
different email address to receive notifications, for example if you want all notifications you create to go to a distribution list. You must also decide if the user will be an Administrator or an unprivileged user. An Administrator has full control over all aspects of the FireAMP deployment. If you uncheck the Administrator box the user will only be able to view data for groups you assign to them. You can also change the user’s privileges later by editing their account. See Access Control for more details.

When you select a user account you can also view the Subscriptions for that user. The Subscriptions list displays any events and reports they have subscribed to.

Time Zone Settings

You can change the time zone displayed by the FireAMP Console for your user account by clicking My Account or going to the Users page and clicking on your Name or Email.
Address. You can change the time zone settings at any time by going back to your account page.

If you need to see a date in UTC or other formats click on the date and a pop-up menu will show other date options. You can also click Change Time Zone to go directly to your user edit page.

**IMPORTANT!** All Connector events will be displayed in the time zone you set and not in the local time zone of the computer that observed the event.

### Access Control

There are two types of users in FireAMP, 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 FireAMP deployment. Administrators can view data from any group or computer in the organization and make changes to groups, policies, lists, and users.
Only administrators can do the following:

- Create and edit Groups.
- Create Policies.
- Access the File Repository and fetch remote files.
- Upload endpoint IOCs.
- Initiate endpoint IOC scans.
- Generate and view Reports.
- Create new users.
- Edit existing users.
- Change user permissions, including granting or revoking administrator permissions.
- Change Business settings.
- Enable Demo Data.
- View the Audit Log.
- Access the Quick Start.

**IMPORTANT!** An administrator can demote another administrator to a regular user but cannot demote themselves.
Unprivileged Users

An unprivileged or regular user can only view information for groups they have been given access to. Certain menu items will not be available to them such as Endpoint IOC scans, File Repository, and Reports.

When you create a new user you will have the choice whether to grant them administrator privileges. If you do not grant them those privileges, you can select which groups, policies, and lists they have access to.

Start by selecting the groups you want the user to have access to. The Clear button removes all groups that have been added to that user. To undo changes from the current session, use the Revert Changes button. The Remove All Privileges button will remove all Groups, Policies, and Outbreak Control lists that have been assigned to the user.

The user will be able to view these groups on the Groups page but not be able to make any changes or create new groups. The user will also be able to view information from FireAMP Connectors in these groups, such as:

- Dashboard Overview Tab, Events Tab, Heat Map Tab
- File Trajectory
- Device Trajectory
- File Analysis
- Threat Root Cause
- Prevalence
- Vulnerable Software
- IOC scans

Once you have selected the groups the user can access you can select the Policies they are allowed to view and edit. You can either manually assign individual policies to the user or click one of the auto-select buttons to populate the policies and outbreak control lists associated with the groups you selected. The Clear button will remove all policies the user has been given access to.

Next you can select Outbreak Control lists the same way. Either select individual lists or click the auto-select button to populate the outbreak control lists assigned to the
policies you previously selected. The **Clear** button next to each list will remove only the lists of that type that have been assigned to the user.

**WARNING!** Exercise caution when assigning access to policies and lists. Some policies and lists can be used by other groups that the user does not have access to. This could allow the user to make changes that affect those groups.

You can also modify a user’s group access at any time, make them an administrator, or demote an administrator to an unprivileged user. When an unprivileged user views their own account they can view the list of groups they can access and change their own password, email addresses, or enable two-step verification.

**IMPORTANT!** When changing user permissions some data is cached in Search results so a user may still be able to see it for a period of time even though they no longer have access to a group. In most cases the cache is refreshed after 5 minutes.

**Two-Step Verification**

Two-step verification provides an additional layer of security against unauthorized attempts to access your FireAMP console account. It uses an RFC 6238 compatible application such as Google Authenticator to generate one-time verification codes to be used in conjunction with your password.

You can enable two-step verification for your account by clicking on **Enable** next to the Two-Step Verification entry on your account in the Users page.

You will then be guided through the steps to enable two-step verification on your account, including backup codes. It is important to keep a copy of your backup codes.
in a safe location in case you are unable to access the device with your authenticator app.

**IMPORTANT!** Each backup code can only be used one time. After you have used all your backup codes you should return to this page to generate new ones.

Once you have successfully enabled two-step verification on your account you will now see a link to view **Two-Step Verification Details**.

If you need to disable two-step verification or generate new backup codes, click this link to return to the two-step verification setup page.

The next time you log in to the FireAMP console you will be prompted for your verification code after you enter your email address and password.
Checking **Remember this computer for 30 days** will set a cookie that allows you to bypass two-step verification on the current computer for the next 30 days. Your browser must be set to allow cookies to use this setting.

**WARNING!** If you accidentally check **Remember this computer for 30 days** on a public computer, a computer you will no longer have access to, or decide to disable two-step verification you should clear the cookies on your browser.

If you do not have access to your authenticator device, click **Can't log in with your verification code?** and enter one of your backup codes that you generated.

If you do not have access to your authenticator device or your backup codes you will need to [contact Support](mailto:contactsupport@fireamp.com).

**API Credentials**

The API Credentials page allows you to add and remove API credentials for specific applications. For more information see the [FireAMP API documentation](https://fireamp.com/docs/api).

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.

[API Credentials interface](https://fireamp.com/docs/api/

**IMPORTANT!** An API credential with read and write scope can make changes to your FireAMP configuration that may cause significant problems with your endpoints. Some of the input protections built into the FireAMP Console do not apply to the API.

The unique API Client ID and API Key for the application will be displayed when you click the Create button. This information cannot be displayed after you leave this page.
so if you forget the credentials or need to change them you will have to delete the credentials and create new ones.

**IMPORTANT!** Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

---

### Business

The Business screen allows you to specify global defaults for your FireAMP deployment and displays your current license status.

Selecting the Default Group or Default Policy from this screen will open the appropriate screen to view the details of the group or policy and edit them if desired. Click the edit link to make changes.

#### Default Group: Audit

The default group is used only if the installation is not associated with another group, or if the group the installation is associated with was deleted.

#### Default Product Policies

A default policy is required by each product when creating a new group. It is also the policy applied if no other policy is inherited or applies.

- FireAMP Windows Audit Policy
- FireAMP Mac Audit Policy for FireAMP Mac
- FireAMP Linux Audit Policy for FireAMP Linux

#### Default Product Versions

The default product version is used to select a product version during installation if no other product version applies.

- FireAMP Windows Latest
- FireAMP Mac Latest
- FireAMP Linux Latest

The Name entry appears on all reports that are generated from your FireAMP deployment. You can also change the Default Group that computers not assigned a group will be a part of. Similarly, the Default Policy defines the initial policy for any new groups that are created unless one is specified or they inherit one through their parent. The Default Product Version allows the administrator to specify which version of the FireAMP Connector will be installed during new deployments.
The Features section of the Business page allows you to enable or disable certain features.

### Features

Status of the features available across your business.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Fetch</td>
<td>On</td>
</tr>
<tr>
<td>3rd Party API Access</td>
<td>Configure API Credentials View API Documentation</td>
</tr>
</tbody>
</table>

### Cisco AMP Threat Grid API

The Cisco AMP Threat Grid API allows you to submit files for analysis. If you already have a Threat Grid account you can enter your API key to link your accounts. You can also select the default virtual machine operating system to be used for analysis.

*VM Image for analysis: Windows XP*

You can disable the Remote File Fetch feature on this screen. To disable it you will need Two-Step Verification enabled on your account and provide your verification code.

**WARNING!** Disabling Remote File Fetch will affect all FireAMP users in your business. To enable it again you will need to contact Support.

### 3rd Party API Access

3rd Party API Access allows you to use the application programming interfaces to access your FireAMP data and events without logging into the Console. You can generate the API Key from the API Credentials page. For more information see the FireAMP API documentation.

You can set the default operating system that files submitted for analysis to your AMP Threat Grid appliance 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
Your current license information is displayed on the right side of the Business screen. The License State indicates whether or not your license is compliant, while License Start and License End display the duration of your current FireAMP license. Seats indicates how many of the seats (FireAMP Connector deployments) you have licensed are currently in use.

Audit Log

The audit log allows the FireAMP administrator to track administrative events within the console that may affect other console users. Actions such as account creations, deletions, password resets, user login, user logout, creation and deletion of reports, policy changes, and other actions are all tracked. Associated information with each entry includes the date, the object acted on, action, changes that were made (if applicable), messages associated with the action, the user who triggered the action, and the IP address they were connected from.

You can filter the audit log to show certain event types, date ranges, users, or IP addresses. The Type includes items such as policies, groups, outbreak control lists, and users. Once you select a Type you can select an Event specific to the event Type.
like creation, deletion, and updates. The Item includes specific lists, computers, groups, and users.

**IMPORTANT!** Item lists with more than 5000 computers cannot be displayed in the pull down menu. Go to Computer Management and locate the computer you want to see the audit log for using the filters, then click the View Changes link for that computer to see a filtered view of the audit log.

Each audit log event can be expanded to show more information on the specific event including the user who generated the event, the IP address of the computer they were logged into at the time, and the time and date.

---

**Demo Data**

Demo Data allows you to see how FireAMP 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 FireAMP Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, Detections, and Events behave when malware is detected. Demo Data can coexist with live data from your FireAMP 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 Demo 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 the Demo Data is enabled, refreshing it will simply refresh all the events so that they appear in the current day's events.

**IMPORTANT!** It can take up to one hour for Demo Data to appear in the Incidents of Compromise dashboard widget. If you disable Demo Data before it has finished populating some events may still appear afterward. You will need to enable Demo Data again then wait at least an hour before disabling it to remove these events.
Applications

The Applications menu shows which applications external to FireAMP that you have authorized to access your organization’s data. For example, you can display FireAMP data in your Cisco Defence Center dashboard. For more information on Defence Center integration with FireAMP see your Defence Center documentation.

From this page you can view your application settings by clicking on its name, edit the groups that are sending data to the application, or deregister the application from FireAMP 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 FireAMP 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 FireAMP entirely you must deregister it from the main Applications screen.
FireAMP has unique network detection event types and Indications of Compromise. Descriptions of these detection types are found in this section.

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

**Indications of Compromise**

FireAMP calculates devices with Indications of Compromise based on events observed over the last 7 days. Events such as malicious file detections, a parent file repeatedly downloading a malicious file (Potential Dropper Infection), or multiple parent files downloading malicious files (Multiple Infected Files) are all contributing factors. Indications of compromise include:

- Threat Detected - One or more malware detections were triggered on the computer.
- Potential Dropper Infection - Potential dropper infections indicate a single file is repeatedly attempting to download malware onto a computer.
- Multiple Infected Files - Multiple infected files indicate multiple files on a computer are attempting to download malware.
- Executed Malware - A known malware sample was executed on the computer. This can be more severe than a simple threat detection because the malware potentially executed its payload.
- Suspected botnet connection - The computer made outbound connections to a suspected botnet command and control system.
- [Application] Compromise - A suspicious portable executable file was downloaded and executed by the application named, for example Adobe Reader Compromise.
Threat Descriptions

DFC Detections

• [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 - An executable file was downloaded from an IP address using a non-standard port. This is often indicative of malware droppers.
• 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.

IMPORTANT! In certain cases the activities of legitimate applications may trigger an Indication of Compromise. The legitimate application is not quarantined or blocked, but to prevent another Indication of Compromise being triggered on future use you can add the application to Application Control - Whitelisting.

DFC Detections

Device Flow Correlation allows you to flag or block suspicious network activity. You can use Policies to specify FireAMP Connector behavior when a suspicious connection is detected and also whether the Connector should use addresses in the Cisco Intelligence Feed, custom IP lists you create, or a combination of both. DFC detections include:

• DFC.CustomIPList - The computer made a connection to an IP address you have defined in a DFC IP Black List.
• Infected.Bothost.LowRisk - The computer made a connection to an IP address thought to belong to a computer that is a known participant in a botnet.
• CnC.Host.MediumRisk - The computer made a connection to an IP address that was previously known to be used as a bot command and control channel. Check the Device Trajectory for this computer to see if any files were downloaded and subsequently executed from this host.
• ZeroAccess.CnC.HighRisk - The computer made a connection to a known ZeroAccess command and control channel.
• Zbot.P2PCnC.HighRisk - The computer made a connection to a known Zbot peer using its peer-to-peer command and control channel.
• Phishing.Hoster.MediumRisk - The computer made a connection to an IP address that may host a phishing site. Often, computers phishing sites also host many other websites and the connection may have been made to one of these other benign sites.
The following supporting documents are available for download.

**Cisco FireAMP Private Cloud Console User Guide**

The current version of the FireAMP Console User Guide can be downloaded here.

*Download the User Guide*

**Cisco FireAMP Private Cloud User Guide**

The current version of the Administration Portal User Guide can be downloaded here.

*Download the Administration Portal User Guide*

**Cisco FireAMP Private Cloud Quick Start Guide**

This guide walks through setting up groups, policies, and exclusions then deploying FireAMP Connectors. This guide is useful for evaluating FireAMP.

*Download the Quick Start Guide*

**Cisco FireAMP Private Cloud Deployment Strategy Guide**

This guide provides a more detailed look at preparing and planning for a production deployment of FireAMP along with best practices and troubleshooting tips.

*Download the Deployment Strategy Guide*
Supporting Documents
Cisco Endpoint IOC Attributes

Cisco Endpoint IOC Attributes
The Endpoint IOC Attributes document details IOC attributes supported by the Endpoint IOC scanner included in the FireAMP Connector. Sample IOC documents that can be uploaded to your FireAMP Console are also included.
Download the Endpoint IOC Attributes

Cisco FireAMP Private Cloud Release Notes
The Release Notes contain the FireAMP change log.
Download the Release Notes

Cisco FireAMP Demo Data Stories
The Demo Data stories describe some of the samples that are shown when Demo Data is enabled in FireAMP.
Download the SFEICAR document
Download the ZAccess document
Download the ZBot document
Download the CozyDuke document
Download the Upatre document
Download the PlugX document
Download the Cryptowall document
Download the Low Prevalence Executable document
A

Access Control 132
Adding Computers 60
Administrators 132
Antivirus Compatibility Using Exclusions 28
Application Blocking TTL 44, 50, 56
Application Control - Blocking 21
Application Control - Whitelists 22
Audit Log 140
Automated Crash Dump Uploads 36
Automatic Signature Updates 45
Available 116

B

Being Processed 116
Browse events for this computer 64
Build a Database from Signature Set. 20
Business 138

C

Clean Cache TTL 44, 50, 56
Cloud Communication Port 39, 48
Cloud Notifications 38, 47
CnC.Host.MediumRisk 145
Common Vulnerabilities and Exposures 125
Common Vulnerability Scoring System 125
Computer Management 63
Connector Log Level 35, 46, 52
Connector Protection 35
Connector User Interface 73
Created By 106
Custom Detections - Advanced 19
Custom Detections - Simple 18

D

Data Source 45
Deepscan Files 45
Demo Data 141
Deployment Summary 63
Detection Action 45, 52, 58
Detection Threshold per ETHOS Hash 43

G

General > Administrative Features 35, 46
General > Client User Interface 37, 46

Index

Detection Threshold per SPERO Tree 43
DFC.CustomIPList 145
Disable Demo Data 141
Download Policy XML File 58

E

Editing IP Blacklists and Whitelists 25
Enable Demo Data 141
Enable DFC 45, 52, 57
End Update Window 37, 48, 54
Entry Point 106
ETHOS 40
Event Disposition 112
Event Flags 112
Event History 110
Event Type 112
Events Tab 13
Exclusions 26
Executed Malware 144
Export to CSV 16

F

Failed 116
Fetch File 115
File > Cache Settings 43, 49
File > Cloud Settings 43
File > Engines 40, 50
File > ETHOS 42, 50
File > Modes 41, 49
File > Scheduled Scans 42, 50
File > TETRA 44
File Conviction Mode 41, 49
File Trajectory 105
File Type 112
Filters 112
Filters and Search 112
Filters and Subscriptions 13
Firewall Connectivity 67
General > Connector Identity Persistence 39
General > Product Updates 36, 48
General > Proxy Settings 38, 47
Generic IOC 145

H
Heartbeat Interval 35, 46, 52
Heat Map Tab 16
Hide File Event Notification from Users 38, 47, 52
Hide Network Notification from Users 38, 47, 52
History 75

I
Identity Synchronization 39
Incompatible software and configurations 67
Indications of Compromise 11, 111
Infected.Bothost.LowRisk 145
Installer 69
Installer Command Line Switches 72
Installer Exit Codes 73
Interactive Installer 69
IP Blacklists 23
IP Whitelists 24

L
List View 15

M
Malicious Cache TTL 44, 50, 56
Malware and Network Threat Detections 13
Menu 7
Monitor File Copies and Moves 41, 49
Monitor Process Execution 41, 49
Multiple Infected Files 144

N
Network - IP Blacklists & Whitelists 23
Network > Device Flow Correlation (DFC) 45, 51

O
Offline Engine 40, 50
On Copy Mode 41, 49
On Copy/Move 42
On Execute 42
On Execute Mode 41, 49
On Move Mode 41, 49
On Scan 42
Overview Tab 11

P
PAC URL 39, 47, 53
Parent Menu 60
Parent menu 60
Phishing.Hoster.MediumRisk 145
Policy Contents 33
Policy Menu 60
Policy menu 60
Potential Dropper Infection 144
Prevalence 122
Product Version 36, 48, 53
Protection Password 35
Proxy Authentication 38, 47, 53
Proxy Autodetection 68
Proxy Hostname 38, 47, 53
Proxy Password 39, 47, 53
Proxy Port 38, 47, 53
Proxy Type 38, 47, 53
Proxy Username 39, 47, 53

R
Reboot 37
Refresh Demo Data 141
Remote File Fetch 139
Requested 116
S

Save Filter As 13
Scan Archives 44
Scan Email 45
Scan Interval 42, 51, 57
Scan Packed 45
Scan Time 42, 51, 57
Scan Type 42, 51, 57
Scanning 74
Scheduled Scan Password 42
Scheduled Scan Username 42, 91
Search 113
Send Filename and Path Info 35, 52
Send Username in Events 35
Settings 75
SHA-256 File Info Context Menu 14
SPERO 40, 49
Start the client user interface 38, 47
Start Update Window 36, 48, 54
Step-Up Enabled 43
Step-Up Threshold 43
Suspected botnet connection 144
Suspicious Cscript Launch 145
Suspicious download 145
System Requirements 7, 65

T

Terminate and quarantine unknown 45
Threat Detected 144
Threat Root Cause 118
Trajectory 108
Tray Log Level 35, 46

U

Uninstall 76
Unknown Cache TTL 44, 50, 56
Unprivileged Users 134
Unseen Cache TTL 44, 56
Update Server 36, 48, 53
Use Proxy Server for DNS Resolution 39, 47, 53
Users 130

V

Verbose Notifications 38
Visibility 106

Z

Zbot.P2PCnC.HighRisk 145
ZeroAccess.CnC.HighRisk 145