Sourcefire FireAMP

User Guide

SOURCEfire®

Version 4.5

Terms of Use Applicable to the User Documentation

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Sourcefire, Inc. or its subsidiaries (collectively, "Sourcefire") or any Sourcefire-provided products. Sourcefire products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

Terms of Use and Copyright and Trademark Notices

Disclaimers

THE DOCUMENTATION AND ANY INFORMATION AVAILABLE FROM IT MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. SOURCEFIRE MAY CHANGE THE DOCUMENTATION FROM TIME TO TIME. SOURCEFIRE MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY SOURCEFIRE-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION. SOURCEFIRE-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND SOURCEFIRE DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SOURCEFIRE BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO SOURCEFIRE-CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF SOURCEFIRE IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

The Documentation may contain "links" to websites that are not created by, or under the control of Sourcefire. Sourcefire provides such links solely for your convenience, and assumes no responsibility for the availability or content of such other sites.

2014-Mar-05 11:44

Table of Contents

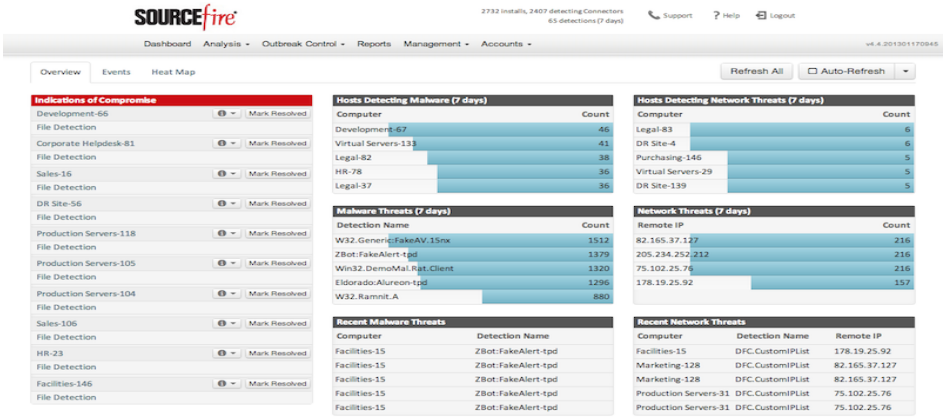
Chapter 1
Introduction

Malware has changed dramatically since the first PC viruses appeared nearly 25 years ago. Today, malware is more sophisticated and evolving faster than ever before so that many organizations find it almost impossible to keep up. Frequently, threats get through various layers of security and into your network without being detected. Sourcefire FireAMP (Advanced Malware Protection) is designed to protect the endpoint layer by not only detecting malware, but also identifying the applications that introduced it. It also allows you to create your own signatures for threats your antivirus does not detect yet and prevent insecure applications from running on your endpoints. Even if FireAMP fails to detect a threat the first time, it can change its mind later on and quarantine all instances of it within your organization.

This document will guide you through the steps needed to properly protect your organization with FireAMP and show you how to use its many advanced features.

CHAPTER 2
DASHBOARD

The Sourcefire 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

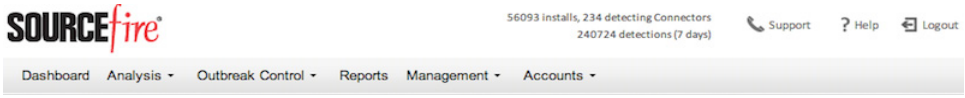
To access the FireAMP Console you will need one of the following Web browsers:

- Microsoft Internet Explorer 10 or higher
- Mozilla Firefox 14 or higher

- Apple Safari 6 or higher
- Google Chrome 20 or higher

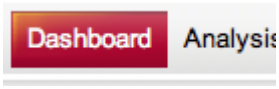
Menu

The menu bar at the top indicates the total number of installs, the number of Connectors detecting malware in the last 7 days, and the number of detections in the last 7 days. Menu items take you to the Dashboard, Analysis, Outbreak Control, Reports, Management, and Accounts as indicated below. It also has a link to contact Sourcefire Support, the Help system and a Logout link to end your session.



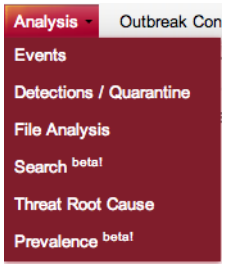
Dashboard

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



Analysis

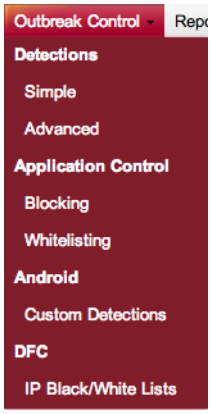
The Analysis menu contains items related to analysis of threats in your environment:



- 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.
- Search to find data from your FireAMP deployment.
- Threat Root Cause to see how malware is getting onto your computers.
- Prevalence to view files that have been executed in your deployment.

Outbreak Control

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



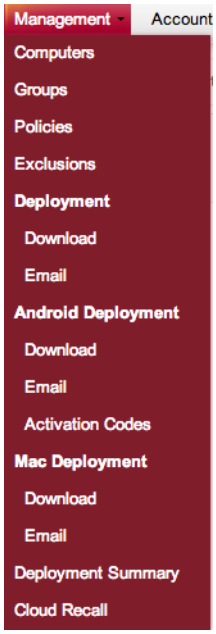
- Detections
  - Simple to convict files that are not yet classified.
  - Advanced to create signatures that will detect parts of the Portable Executable (PE) file.
- Application Control
  - Blocking to stop executables from running.
  - Whitelisting to create lists of applications that will not be wrongly detected.
- Android
  - Custom Detections to warn of new threats or unwanted apps.
- DFC
  - IP Black/White Lists to explicitly detect or allow connections to specified IP addresses.

Reports

The Reports link allows you to create PDF reports based on your data.

Management

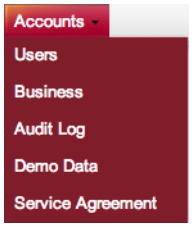
The Management menu contains items that allow you to manage your FireAMP Connectors.



- 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.
- Deployment
  - Download to download the FireAMP Windows Connector.
  - Email to email links to download the FireAMP Windows Connector.
- Android Deployment
  - Download to download the FireAMP Mobile Connector.
  - Email to email links to download the FireAMP Mobile Connector.
  - Activation Codes to authorize mobile devices.
- Mac Deployment
  - Download to download the FireAMP Mac Connector.
  - Email to email links to download the FireAMP Mac Connector.
- Deployment Summary to view deployment failures.
- Cloud Recall™ to approve items that are not automatically taken care of by Cloud Recall™.

Accounts

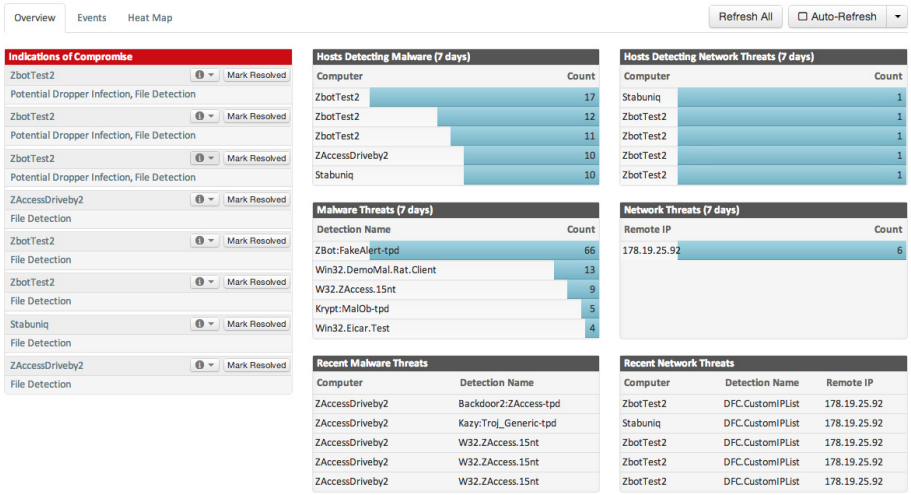
The Accounts menu contains items related to FireAMP console accounts:



- Users to view and create users.
- Business to set the company name, default group and default policy, and view license information.
- Audit Log to see changes to your account.
- Demo Data to populate your console with sample events.
- 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.
- Service Agreement displays the Sourcefire FireAMP products subscription agreement.

Overview Tab

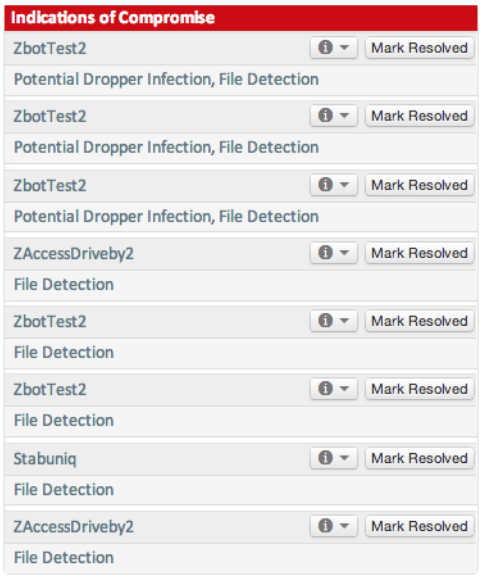
The **Overview** tab is composed of multiple widgets highlighting recent malicious activity in your FireAMP deployment. The tab is divided into three types of information: Indications of Compromise, malware detections, and network threats.



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.

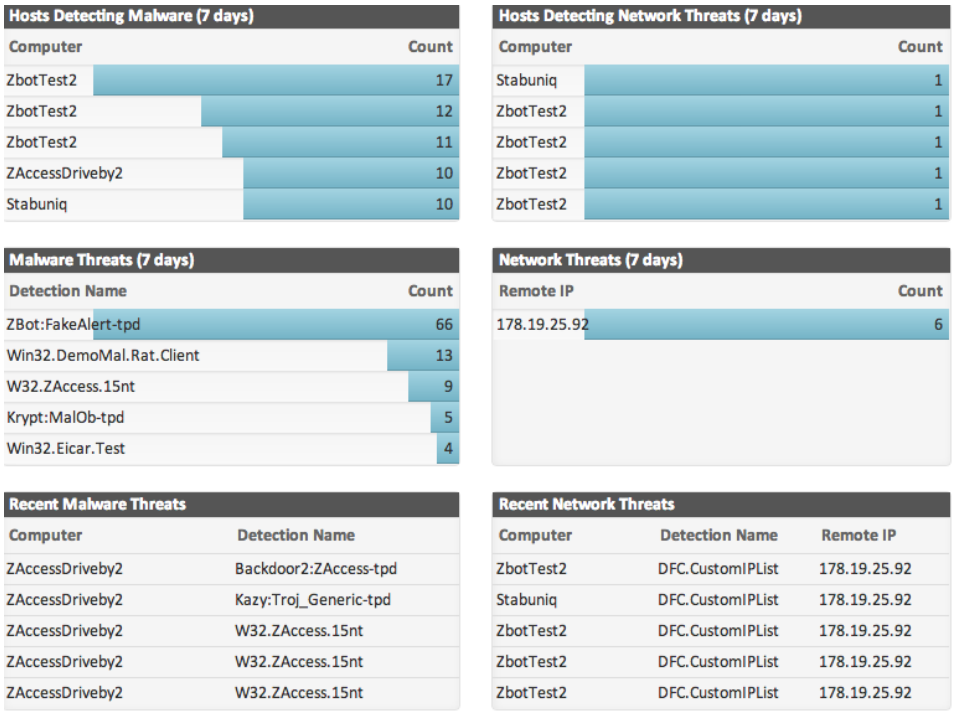


FireAMP calculates devices with Indications of Compromise based on events observed over the last 7 days. Events such as malicious file detections, a parent file repeatedly downloading a malicious file (Potential Dropper Infection), or multiple parent files downloading malicious files (Multiple Infected 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 File Trajectory. 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.



Hosts Detecting Malware (7 days)

Computer	Count
ZbotTest2	17
ZbotTest2	12
ZbotTest2	11
ZAccessDriveby2	10
Stabuniq	10

Hosts Detecting Network Threats (7 days)

Computer	Count
Stabuniq	1
ZbotTest2	1
ZbotTest2	1
ZbotTest2	1
ZbotTest2	1

Malware Threats (7 days)

Detection Name	Count
ZBot:FakeAlert-tpd	66
Win32.DemoMal.Rat.Client	13
W32.ZAccess.15nt	9
Krypt:MalOb-tpd	5
Win32.Eicar.Test	4

Network Threats (7 days)

Remote IP	Count
178.19.25.92	6

Recent Malware Threats

Computer	Detection Name
ZAccessDriveby2	Backdoor2:ZAccess-tpd
ZAccessDriveby2	Kazy:Troj_Generic-tpd
ZAccessDriveby2	W32.ZAccess.15nt
ZAccessDriveby2	W32.ZAccess.15nt
ZAccessDriveby2	W32.ZAccess.15nt

Recent Network Threats

Computer	Detection Name	Remote IP
ZbotTest2	DFC.CustomIPList	178.19.25.92
Stabuniq	DFC.CustomIPList	178.19.25.92
ZbotTest2	DFC.CustomIPList	178.19.25.92
ZbotTest2	DFC.CustomIPList	178.19.25.92
ZbotTest2	DFC.CustomIPList	178.19.25.92

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.

Events Tab

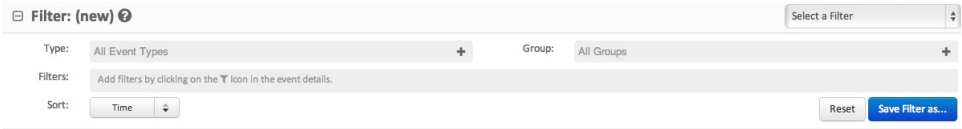
The **Events** tab initially shows the most recent events in your FireAMP deployment. Navigating to the **Events** tab by clicking on a threat, IP address, or computer name in the **Dashboard** tab will provide different filtered views.

Filters and Subscriptions

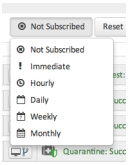
The filters are shown at the top of the Events tab. You can select a previously saved filter from the drop down on the right side or add event types, groups, or specific filters from existing events. To remove a filter criteria, click the x next to the item you want to remove. You can also sort the Events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



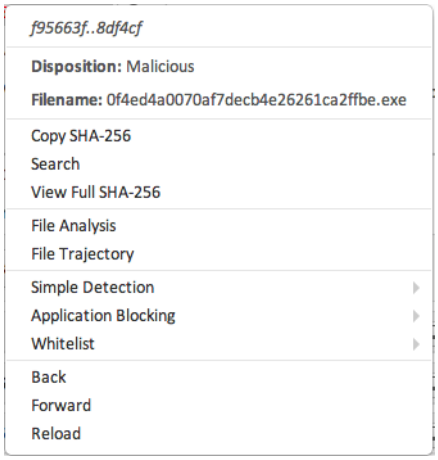
To subscribe to a filter view click the Not Subscribed button to show a menu with subscription timing options. You can subscribe to events with immediate, hourly, daily, weekly, or monthly notifications.



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.



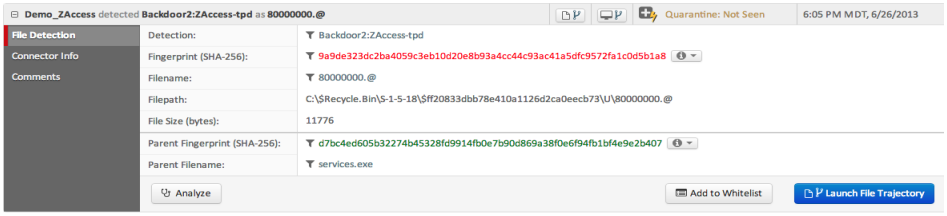
You can copy or view the full SHA-256 value or perform a Search for that SHA-256 to see where else it was seen in your organization. You can also launch File Trajectory for the SHA-256 or submit it for File Analysis. The context menu also

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 Custom Detections, Application Blocking, or Custom Whitelists.

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 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.



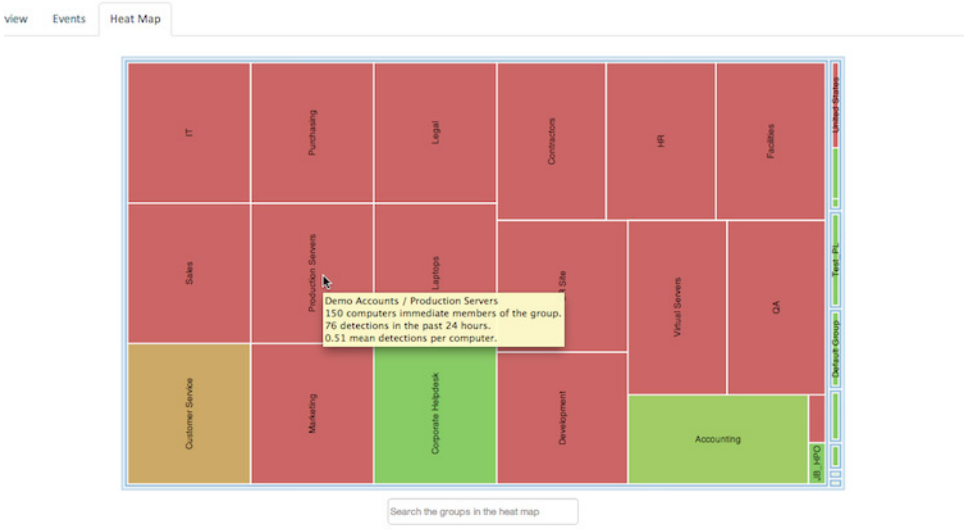
Heat Map Tab

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.

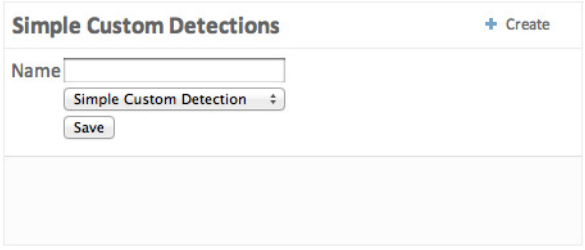
CHAPTER 3
OUTBREAK CONTROL

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, Custom Whitelists, Advanced Custom Signatures, and Exclusion Sets.

Simple Custom Detections

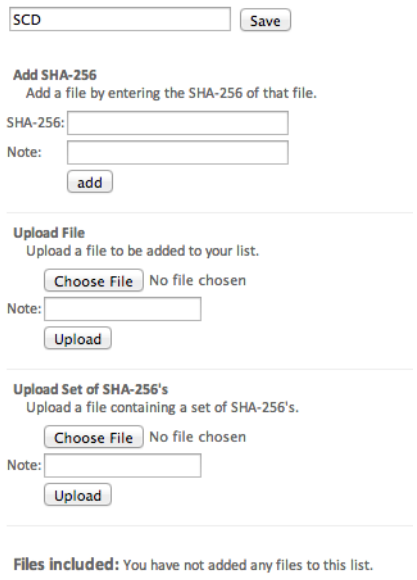
A Simple Custom Detection list is similar to a blacklist. These are files that you want to detect and quarantine. Not only will an entry in the Simple Custom Detection list quarantine future files, but through Cloud Recall™ it will quarantine instances of the file on any endpoints in your organization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

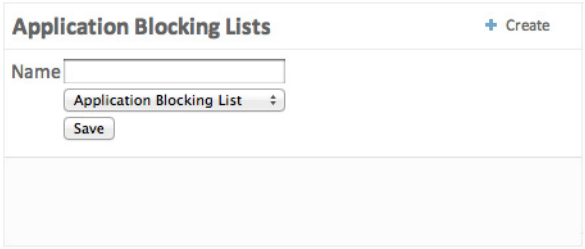
IMPORTANT! You cannot add any file that is on our global whitelist or is signed by a certificate that we have not revoked. If you have found a file that you think is incorrectly classified or is signed and want us to revoke the signer, please email support@sourcefire.com.

Application 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.

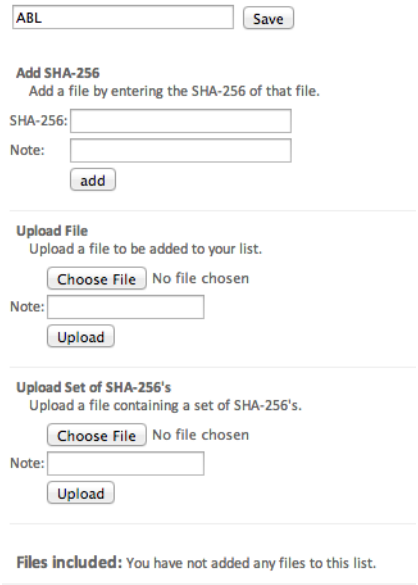
In order to create an Application Blocking list, go to **Outbreak Control > Blocking**. Click **Create** to create a new Application Blocking list, give it a name, and click on **Save**.



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. The SHA-256s and notes can bee seen if you click on the **Files included** link on the bottom right. If you accidentally

added a SHA-256 that you did not want to, click **Remove**. You can also edit the name of the list and click **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.

Advanced Custom Signatures

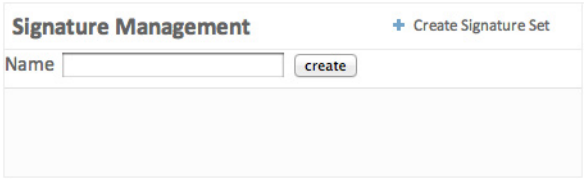
Advanced Custom Signatures are like traditional antivirus signatures, but they are written by the user. These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:

- MD5 Signatures

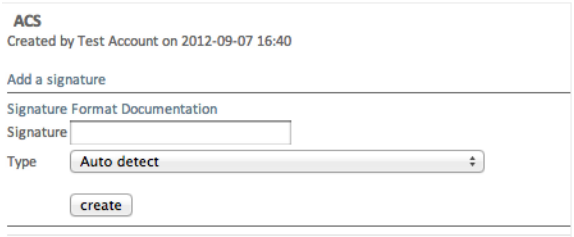
- MD5, PE section based Signatures
- File Body-based Signatures
- Extended Signature Format (offsets, wildcards, regular expressions)
- Logical Signatures
- Icon Signatures

More information on signature formats can be found at http://www.clamav.net/doc/latest/signatures.pdf. These signatures are compiled into a file downloaded to the endpoint.

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



After you create the Advanced Custom Signature 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 Signature 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

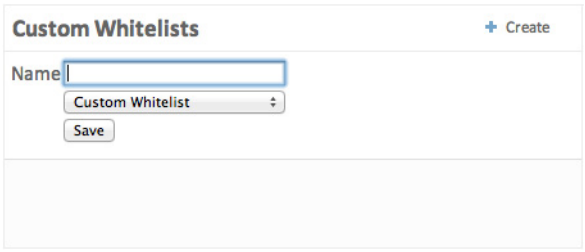
If a file is added to an Advanced Custom Signature the cache time must expire before the detection will take effect. For example, if you add an Advanced

Custom Signature for an unknown file 5 minutes after it was cached, the detection will not take effect for another 55 minutes.

Custom Whitelists

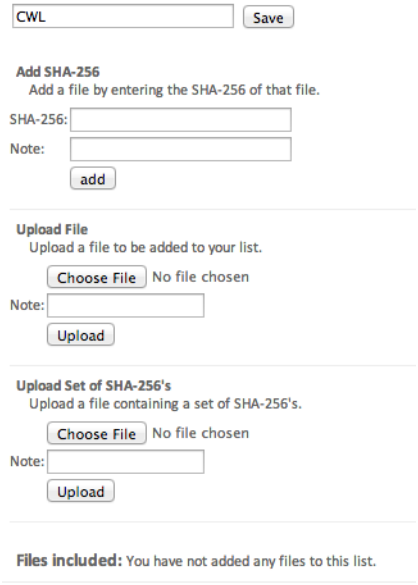
A Custom Whitelist is for files you never want to convict. A few examples of this are a custom application that is detected by a generic engine or a standard image that you use throughout the company.

To create a Custom Whitelist, go to **Outbreak Control > Whitelisting**. Next click **Create** to create a new Custom Whitelist, give it a name, and click **Save**.



After you save the Custom 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. The SHA-256s and notes can bee seen if you click on the **Files included** link on the bottom right. If you added a SHA-256 that you did not want to, click **Remove**. You can also edit the name of the list and click **Save** to rename it.



IP Black / White Lists

IP Black and White Lists 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 Sourcefire 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:

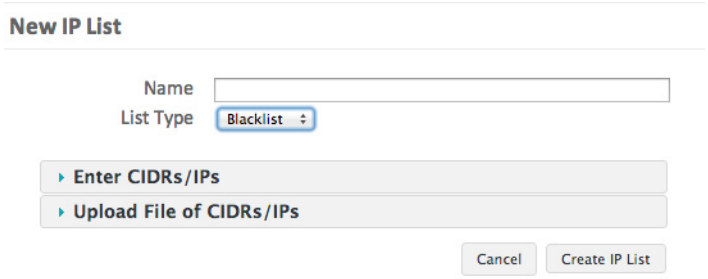
```
0.0.0.1/1:xx
128.0.0.1/1:xx
```

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.

IP Black Lists

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 Black/White Lists** and click **Create IP List**. Give the list a name and select **Black List** 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.

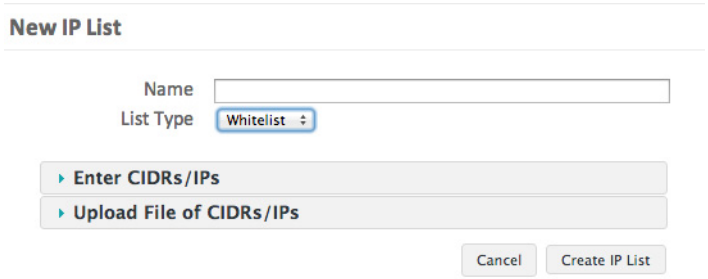


IP White Lists

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 Sourcefire 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 Black/White Lists** and click **Create IP List**. Give the list a name and select **White List** 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 Black / White Lists

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.

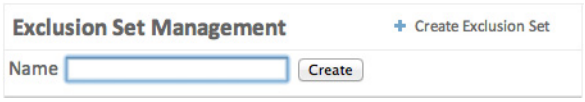
Custom Exclusion Sets

A Custom Exclusion Set is a file location, extension, or threat name that you do not want to scan or convict. For example, if you are running an antivirus product, you will want to exclude the location where that product is installed.

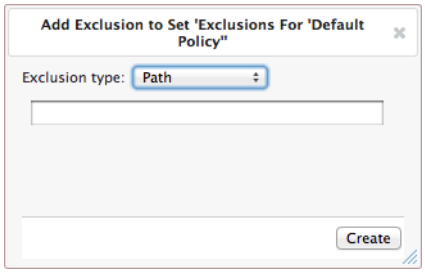
WARNING! Any files located in a directory that has been added to an Exclusion list will not be subjected to Application Blocking, Simple Custom Detections, or Advanced Custom Signature lists.

Creating and Managing Custom Exclusion Sets

To create a Custom Exclusion Set, go to **Management > Exclusions**. Click **Create Exclusion Set**, give it a name, and click **Create**.



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



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 by path, 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.

If you accidentally create an exclusion you do not want, you can click on the header to expand the exclusion and click **Remove** to get rid of it.

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

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

Microsoft ForeFront

- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILESX86\Microsoft Forefont

Microsoft Security Client

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

Sophos

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

Splunk

- CSIDL_PROGRAM_FILES\Splunk

Symantec Endpoint Protection

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

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

Creating Exclusions for the FireAMP Connector in Other 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 MobileFireAMP 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.
4. Edit your On-Access High-Risk Processes Policies.
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.
7. Click OK.
8. Click Save.
9. Edit your On-Access Low-Risk Processes Policies.
10. Repeat steps 5 through 8 for this policy.

Creating Exclusions for the FireAMP Connector in McAfee VirusScan Enterprise 8.8

1. Open the VirusScan Console.
2. Select On-Access Scanner Properties from the Task menu.
3. Select All Processes from the left pane.
4. Select the Exclusions tab.
5. Click the Exclusions button.

6. On the Set Exclusions dialog click the Add button.
7. Click the Browse button and select your 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.
10. Click OK on the On-Access Scanner Properties 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 folder (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 folder (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

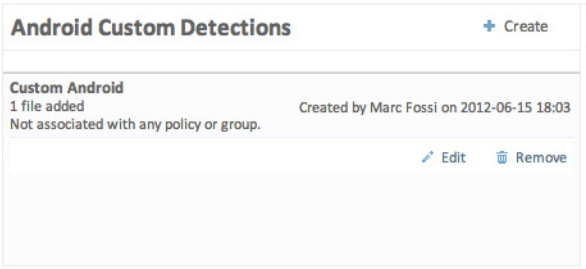
1. Open Microsoft Security Essentials and click on the Settings tab.
2. Select Excluded files and locations in the left pane.
3. Click the Browse button and navigate to your FireAMP Connector installation folder (C:\Program Files\Sourcefire\FireAMP by default) and click OK.
4. Click the Add button then 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.

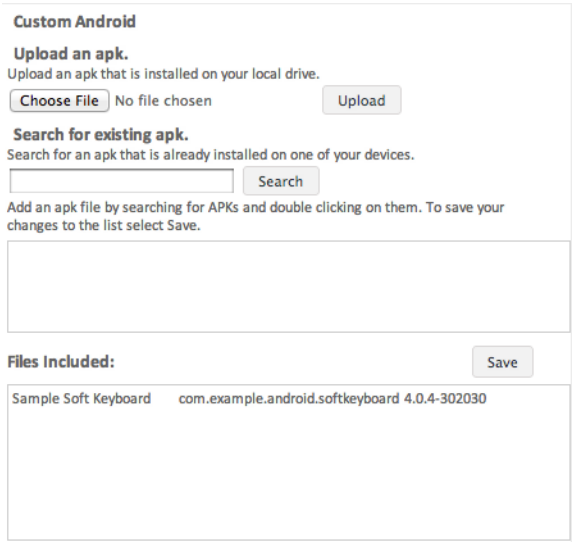
Android Custom Detections

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

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



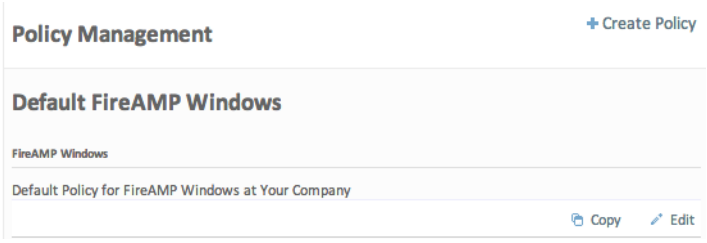
After you save the Android Custom Detection, click on **Edit** and you will see two ways to add values to this list.



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

CHAPTER 4
POLICIES

Now that you have your lists defined, you can combine them with other settings into a policy. A policy is applied to a computer via Groups.

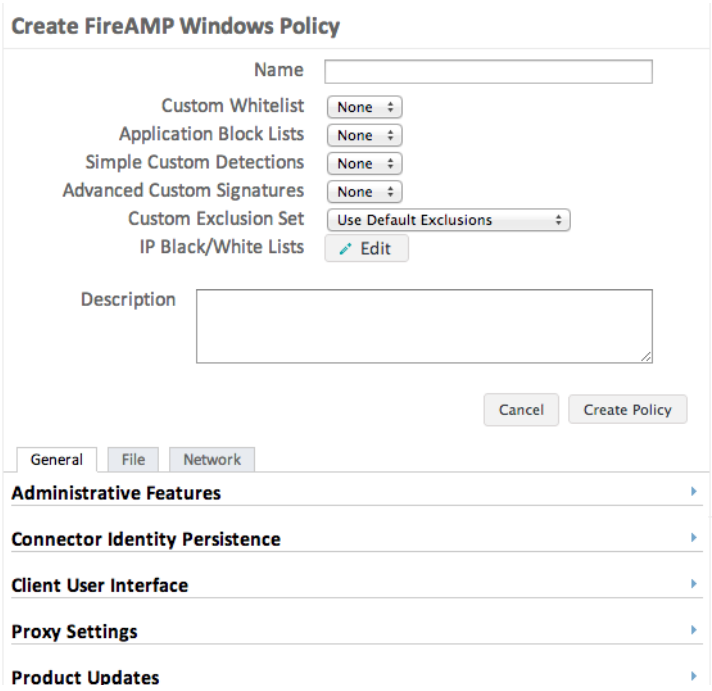


Click **Create Policy** to create a new policy or **Copy** if you want to create a new policy based on an existing one. If you have a FireAMP Mobile license you will be asked to choose the type of policy you want to create.

This will take you to the creation page. The configuration is covered below.

Policy Contents

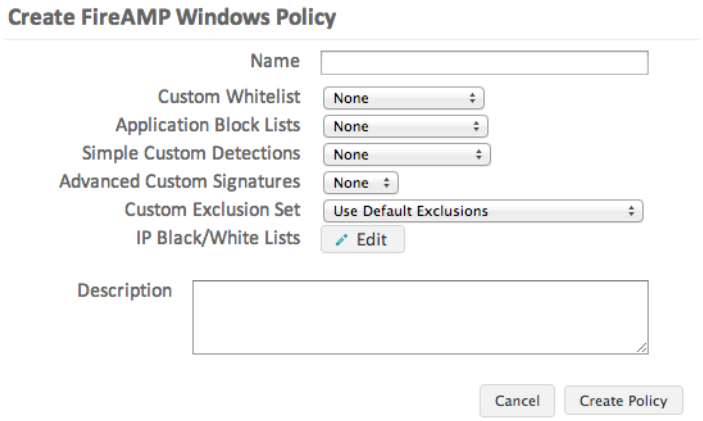
There are numerous settings that can be set in the policy. This section will detail each one. FireAMP Windows and FireAMP Mac both share some basic policy settings



Name, Lists, and Description

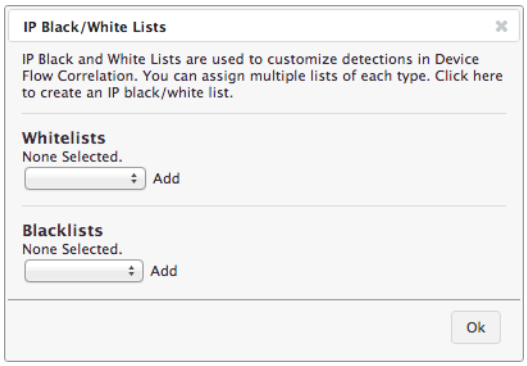
The Name is just a name that you can use to recognize the policy. The Custom Whitelists, Application Blocking, Simple Custom Detections, Advanced Custom Signatures, IP Black Lists, IP White Lists, and Custom Exclusion Sets were

described in the Outbreak Control section of this document. The description can be used to give more description about the policy.



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

When you click IP Black/White Lists **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 White List entries will override IP Black List entries.

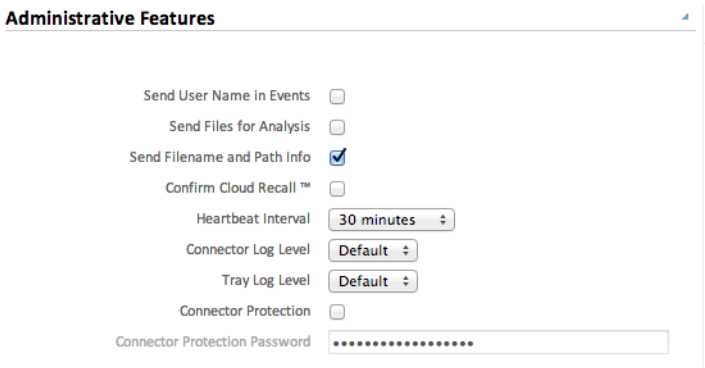
FireAMP Windows Connector

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 username that the process is executed, copied, or moved as. 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 Files for Analysis will send files that FireAMP does not currently have and is required to do further analysis on. This is one way we collect new malware and cleanware samples.

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

Cloud Recall™ is a process in which we review files to make a new determination based on additional information. For example, a new file that has just come out may be classified as unknown. However, two days later, we determine it is malicious. We then find every Connector that has seen that file and attempt to quarantine it when the Connector calls home on its heartbeat interval. Instead of automatically quarantining a file or restoring it from quarantine, **Confirm Cloud Recall™** will allow the administrator to approve each file requested to be restored from quarantine or quarantined.

IMPORTANT! If you have already quarantined a file in your environment through a Simple Custom Detection or Advanced Custom Signature and the file is Recalled, you will not receive Cloud Recall™ confirmations for that file.

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.

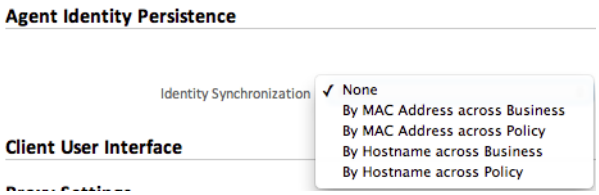
Connector Log Level and **Tray Log Level** allow you to choose between default and debug (verbose) logging levels. The default level should be set unless debug is requested by Sourcefire support during troubleshooting.

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.

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.

General > Connector Identity Persistence



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.

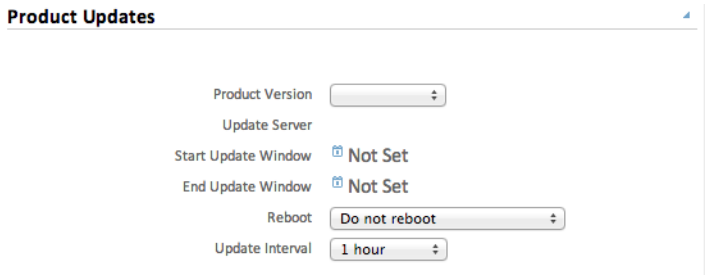
By MAC Address across Policy - New Connectors look for the most recent Connector that has the same MAC address to synchronize with within the same policy.

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.

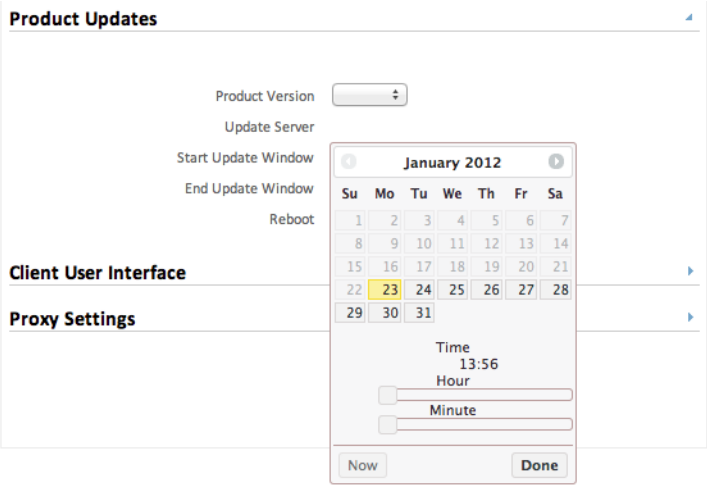
IMPORTANT! In some cases a cloned virtual machine may be placed in the Default Group rather than the group it was cloned from. If this occurs, move the virtual machine into the correct group in the FireAMP Console.

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 every30 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.

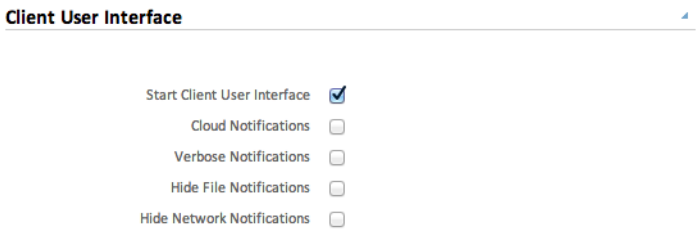
End Update Window allows you to choose a date and time in which the updates will stop occurring.

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.

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.

General > Client User Interface



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

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

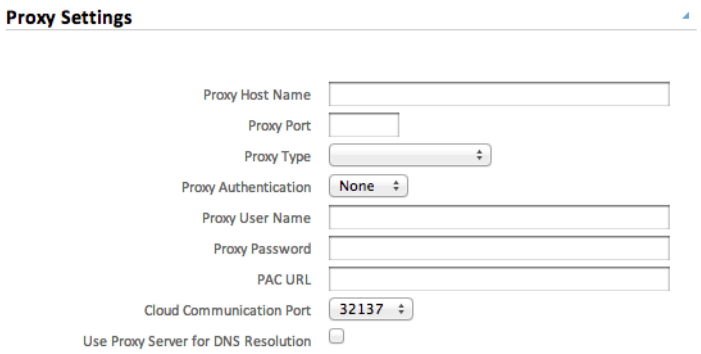
Cloud Notifications are balloon pop-ups that come from the Windows system tray when the FireAMP Connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud.

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 Event Notification from Users suppresses notifications from being displayed to the user when a malicious file is convicted or quarantined by the Connector.

Hide Network Notification from Users suppresses notifications from being displayed to the user 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, SOCKS4, SOCKS4a, SOCKS5, and SOCKS5_hostname.

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

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

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.

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

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

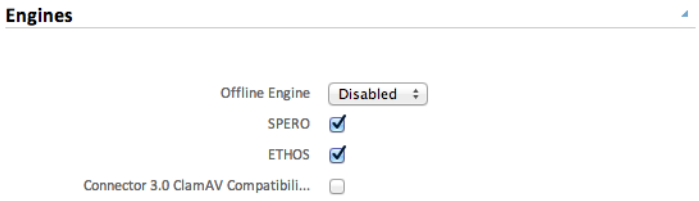
IMPORTANT! The URL must specify HTTP or HTTPS when defined through policy and only ECMAScript-based PAC files with a .pac extension are supported. If the PAC file is hosted on a Web server, the proper MIME type of application/x-javascript-config must be specified.

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

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



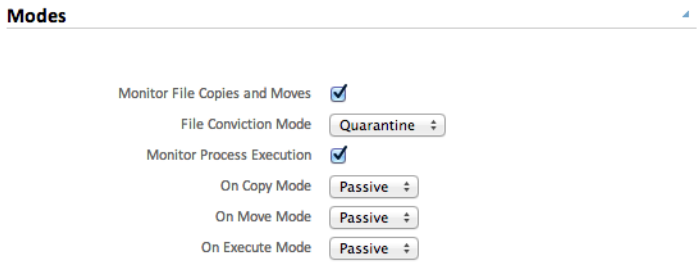
Offline Engine can be set to **Disabled** or **TETRA**. TETRA is a full antivirus replacement and should never be enabled if another antivirus engine is installed. TETRA can also consume significant bandwidth when downloading definition updates, so caution should be exercised before enabling it in a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

SPERO is the Sourcefire 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 Sourcefire 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.

Connector 3.0 ClamAV Compatibility Mode should be used if any Connectors in the group are version 3.0. It allows 3.0 Connectors to download Advanced Custom Signatures and the regular daily Clam definitions.

File > Modes



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

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.

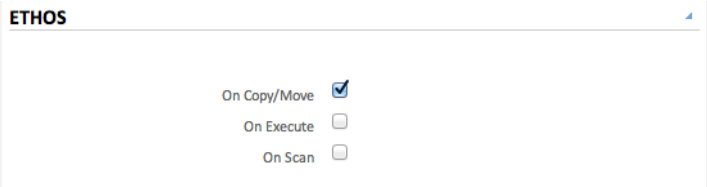
WARNING! When **File Conviction Mode** is set to **Audit** any malicious files on your endpoints will remain accessible and be allowed to execute. Application Blocking Lists will also not be enforced. You should only use this setting for testing purposes with proprietary software.

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

On Copy Mode, **On Move Mode**, and **On Execute Mode** can run in two different modes, Active or Passive. In Active mode, the file is blocked from being copied, moved, or 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 copied, moved, or 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.

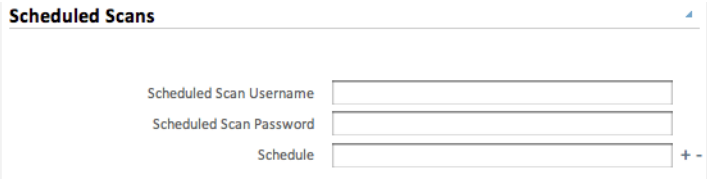
Send Filename and Path Info will send the filename and path information to FireAMP so that they are visible in the Events Tab, Device Trajectory, and File Trajectory. Unchecking this setting will stop this information from being sent.

File > ETHOS



ETHOS is a great engine for grouping files together, but unfortunately it 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

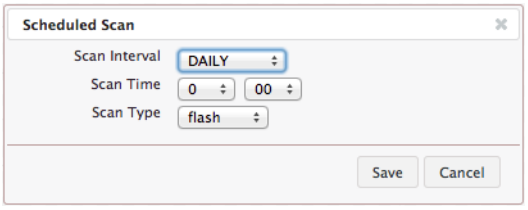


Scheduled scans are not necessary for the operation of the FireAMP Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Cloud Recall™. This allows companies to reduce their energy footprint by eliminating the need for scheduled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

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.

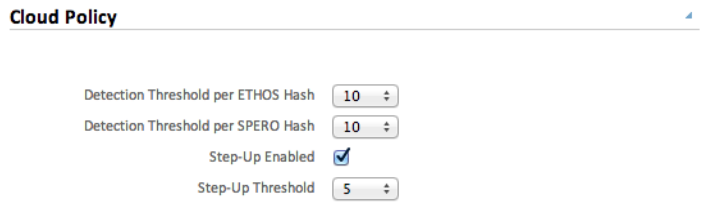


Scan Interval is how often it should run. The options are **Daily**, **Weekly**, or **Monthly**.

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. If TETRA is enabled it will perform a **rootkit** scan as well. A custom scan will scan a particular path that you give it.

File > Cloud Policy



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

SPERO is considered to be a generic engine. Because of this, the user has the ability to control how false positive-prone a 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 Simple Custom Detections list or create Advanced Custom Signatures for it.

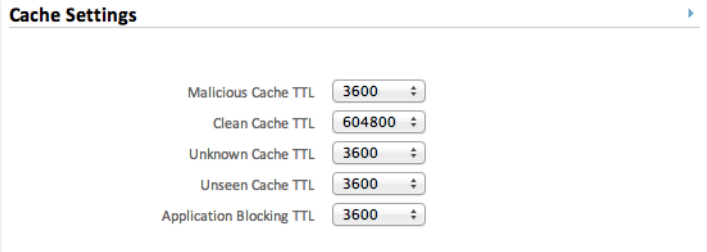
Detection Threshold per SPERO Tree means that a single SPERO tree can convict a single SHA of unknown disposition a maximum number of times. The default is 10 meaning that SPERO will not convict any SHA-256 seen 10 times in 24 hours

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 Simple Custom Detections list or create Advanced Custom Signatures for it.

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

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

File > Cache Settings



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

Malicious Cache TTL is the time in seconds 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.

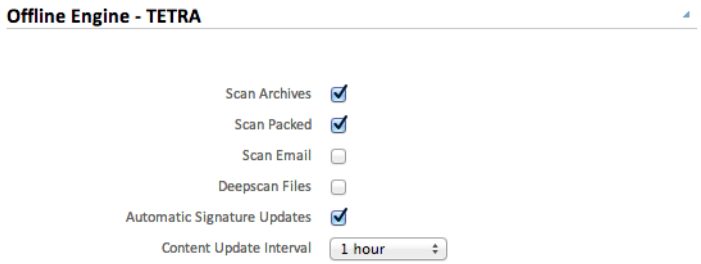
Unknown Cache TTL is the time in seconds that a file with an unknown disposition is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is one hour.

Unseen Cache TTL is the time in seconds that a file that has not previously been observed by the community 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 > 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,

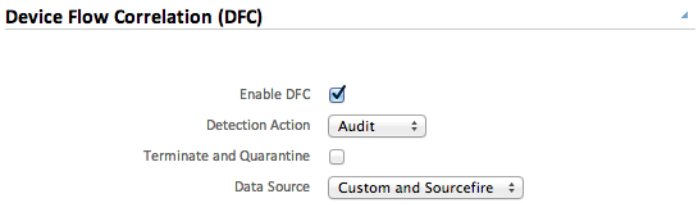
so caution should be exercised before enabling automatic signature updates in a large environment.

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 to 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 unknown 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 **Sourcefire** to have your Connectors only use the Sourcefire Intelligence Feed to define malicious sites. The Sourcefire Intelligence Feed represents IP addresses determined by the Sourcefire 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 Sourcefire** option will allow you to use both the IP Blacklists you have added to the policy and the Sourcefire Intelligence Feed.

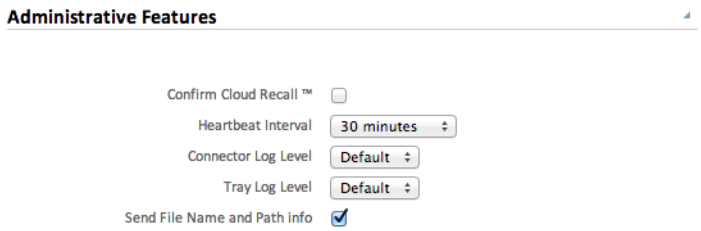
FireAMP Mac Connector

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



Cloud Recall™ is a process in which we review files to make a new determination based on additional information. For example, a new file that has just come out may be classified as unknown. However, two days later, we determine it is malicious. We then find every Connector that has seen that file and attempt to quarantine it when the Connector calls home on its heartbeat interval. Instead of automatically quarantining a file or restoring it from quarantine, **Confirm Cloud Recall**™ will allow the administrator to approve each file requested to be restored from quarantine or quarantined.

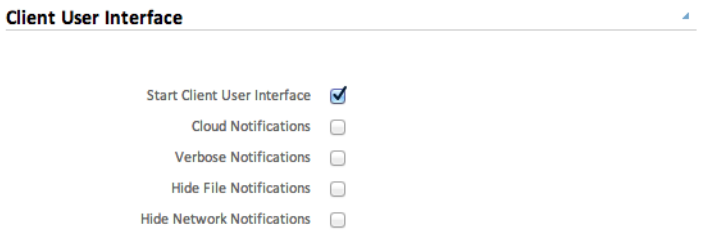
IMPORTANT! If you have already quarantined a file in your environment through a Simple Custom Detection or Advanced Custom Signature and the file is Recalled, you will not receive Cloud Recall™ confirmations for that file.

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 Sourcefire support during troubleshooting.

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

General > Client User Interface



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

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

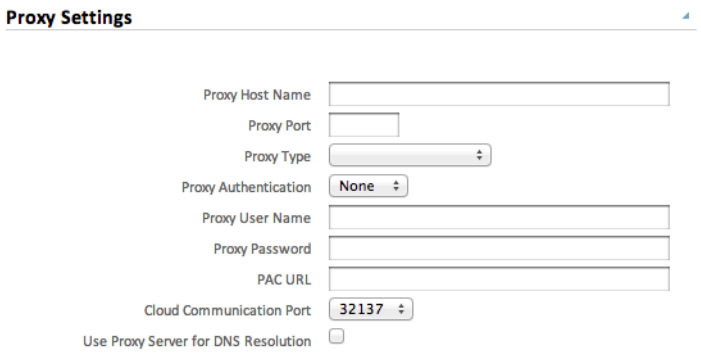
Cloud Notifications are balloon pop-ups that come from the Notification Center when the FireAMP Connector is successfully connected to the cloud. It displays the number of users and detections registered to the cloud.

Verbose Notifications are boxes that pop-up from the Notification Center 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 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 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, SOCKS4, SOCKS4a, SOCKS5, and SOCKS5_hostname.

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

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

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.

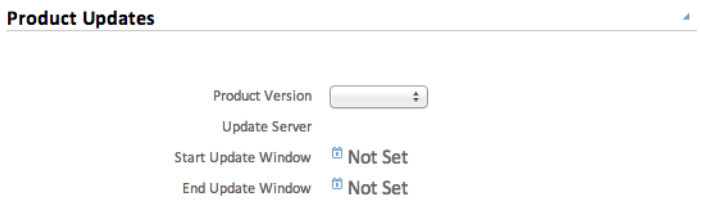
Cloud Communication Port allows you to select whether your Connectors perform cloud lookups on TCP 32137 or 443.

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

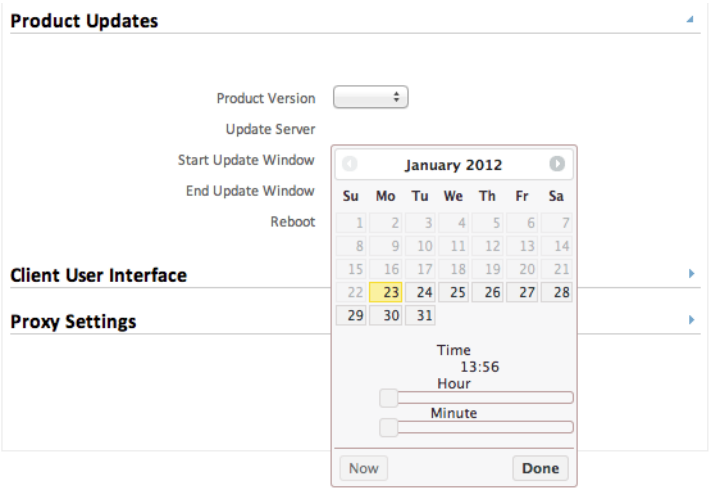
IMPORTANT! The URL must specify HTTP or HTTPS when defined through policy and only ECMAScript-based PAC files with a .pac extension are supported. If the PAC file is hosted on a Web server, the proper MIME type of application/x-javascript-config must be specified.

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

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.

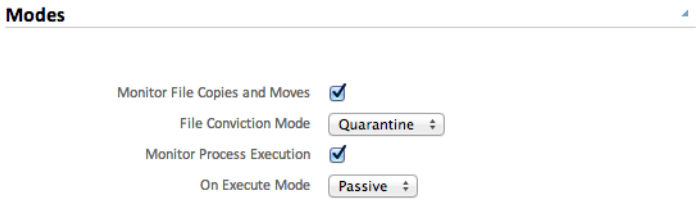
Reboot gives you the options **Do not reboot**, **Ask for reboot** from the user, or **Force reboot after 2 minutes**.

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

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



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

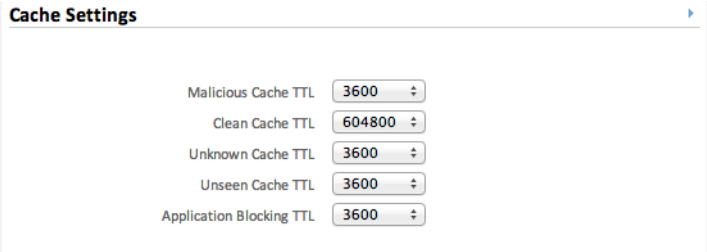
File Conviction Mode allows you to specify the action the Connector takes when a malicious file is convicted. Setting this to Audit will stop the FireAMP Connector from quarantining any files.

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 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.

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.

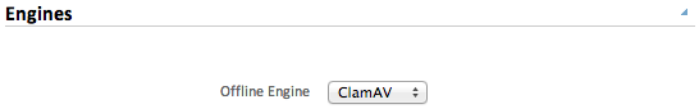
Unknown Cache TTL is the time in seconds that a file with an unknown disposition is cached before another cloud lookup is performed when a Connector sees that SHA-256 value. The default value is one hour.

Unseen Cache TTL is the time in seconds that a file that has not previously been observed by the community 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.

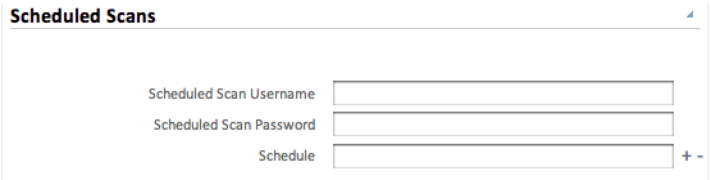
IMPORTANT! If you add a SHA-256 with a clean disposition to an application blocking list that was previously seen by a Connector you must stop the Connector and delete the cache.db file from the installation directory on that computer for the application to be blocked from executing. Otherwise, you will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

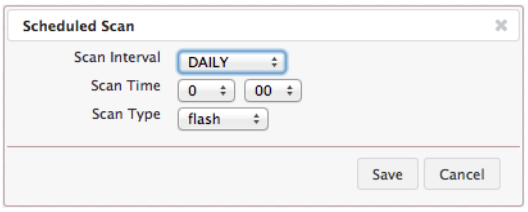


Scheduled scans are not necessary for the operation of the FireAMP Connector because files are being reviewed as they are copied, moved, and executed. Files are also reviewed again for 6 months using Cloud Recall™. This allows companies to reduce their energy footprint by eliminating the need for scheduled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

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 **Daily**, **Weekly**, or **Monthly**.

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

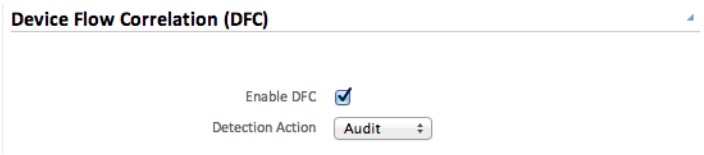
Scan Type is the type of scan. A **flash** scan will scan the processes running and the files and registry entries used by those processes. A **full** scan will scan the

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. If TETRA is enabled it will perform a **rootkit** scan as well. A custom scan will scan a particular path that you give it.

Network Tab

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

Network > Device Flow Correlation (DFC)

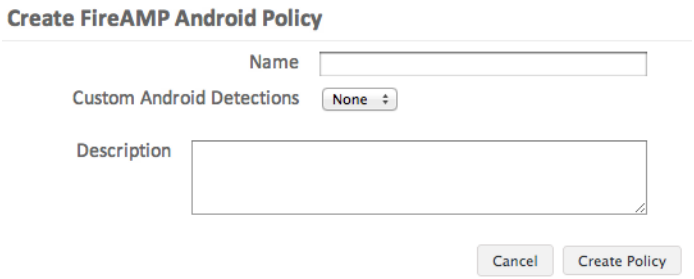


Enable DFC will enable Device Flow Correlation on your FireAMP Connector. This allows you to monitor network activity and determine which action the Connector should take when connections to malicious hosts are detected.

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

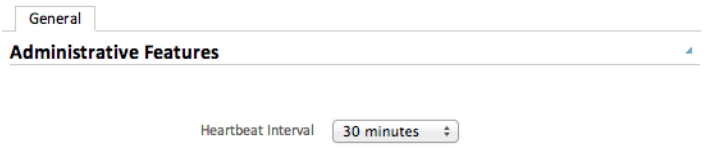
FireAMP Mobile Policy

A policy for the FireAMP Mobile Connector contains fewer options due to the nature of the device.



The **Name** is just a name that you can use to recognize the policy. The Android Custom Detections were described in the Outbreak Control section of this document. The **Description** can be used to give more information about the policy.

Connector > Administrative Features

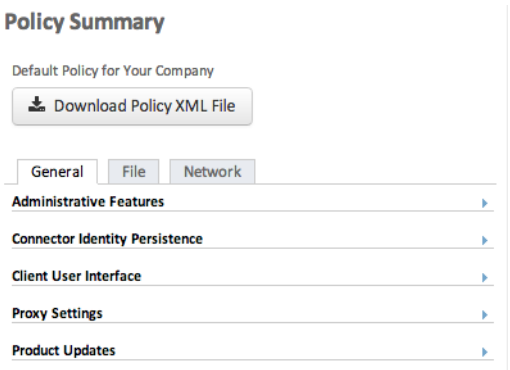


The **Heartbeat Interval** is the interval in which the Connector calls home to see if there are any policies to pick up, new Custom Detections or any tasks to perform such as product updates.

Policy Summary

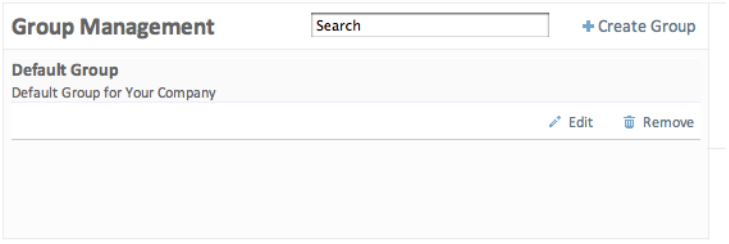
Once you have created policies you can view a summary of each one's contents from the main Policy Management page. Click on the name of the policy you want to view and the summary will be displayed in the right-hand pane.

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.



CHAPTER 5
GROUPS

Now that you have a policy you can create a group that the policy will apply to. 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.

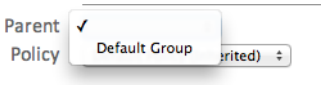
Configuring the Group

This section will take you through the steps to configure the group.

Name and Description

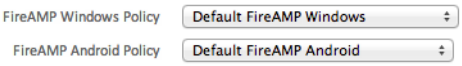
The name and description of the group are simply used to identify it. Groups can frequently reflect geographic locations, business units, user groups, and so on. Groups should be defined according to policies that will be applied to each one.

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.

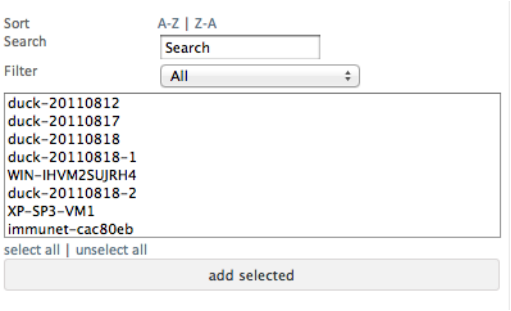
Policy Menu



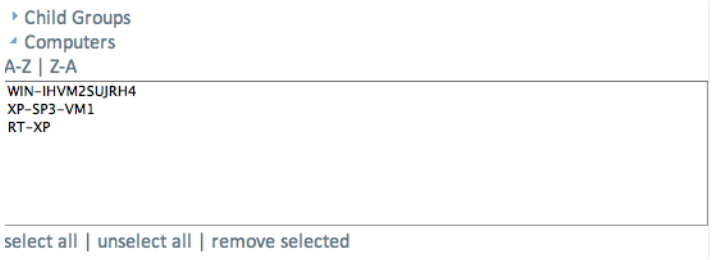
The **Policy** menu allows you to specify which policy to apply to the group you are creating. By default the Default Policy will be applied to the new group unless a parent group has been selected. If a parent has been selected, then the new group will inherit the policy of the parent. Note that if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

If you have a FireAMP Mobile license you will also be able to select the policy for any Mobile Connectors that are part of the group.

Adding Computers



After the name, description, parent, and policy have been specified for the group you can start adding computers to it. The list can be sorted by computer name, searched, or filtered by groups. Note that adding a computer that is already a member of another group to a new group will remove it from the other group and add it to the new one. When you have selected the computers you want added to the group click **add selected**.



The computers that were added will then appear in the window shown above. From here you can remove any computers that were added accidentally.

Moving Computers

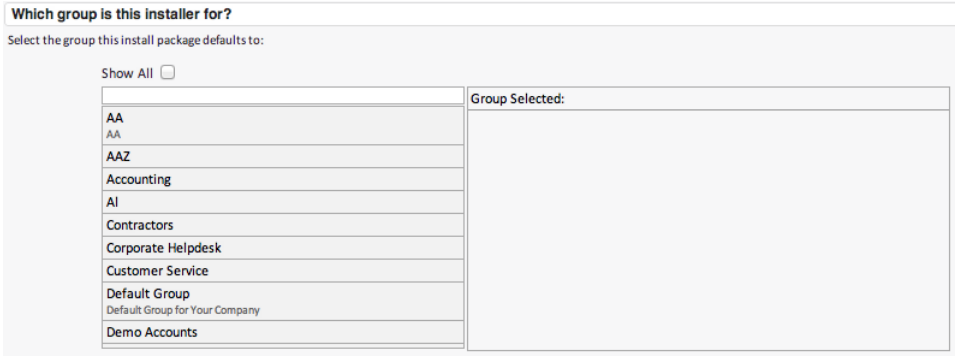
If you want to move computers from one group to another, go to **Management > Groups** and click **Edit** under the *destination* group. In the right pane, select the computers you want to add (you can use Search and Filter to narrow the scope) and click **add selected**. Since computers can only be a member of one group, the computers you add will automatically be removed from their original groups and added to the current group.

CHAPTER 6
DEPLOYING THE FIREAMP WINDOWS CONNECTOR

There are two ways to install the FireAMP Connector on client computers - direct download and email. This section will walk you through both.

Direct Download

The direct download option allows you to 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 create 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.

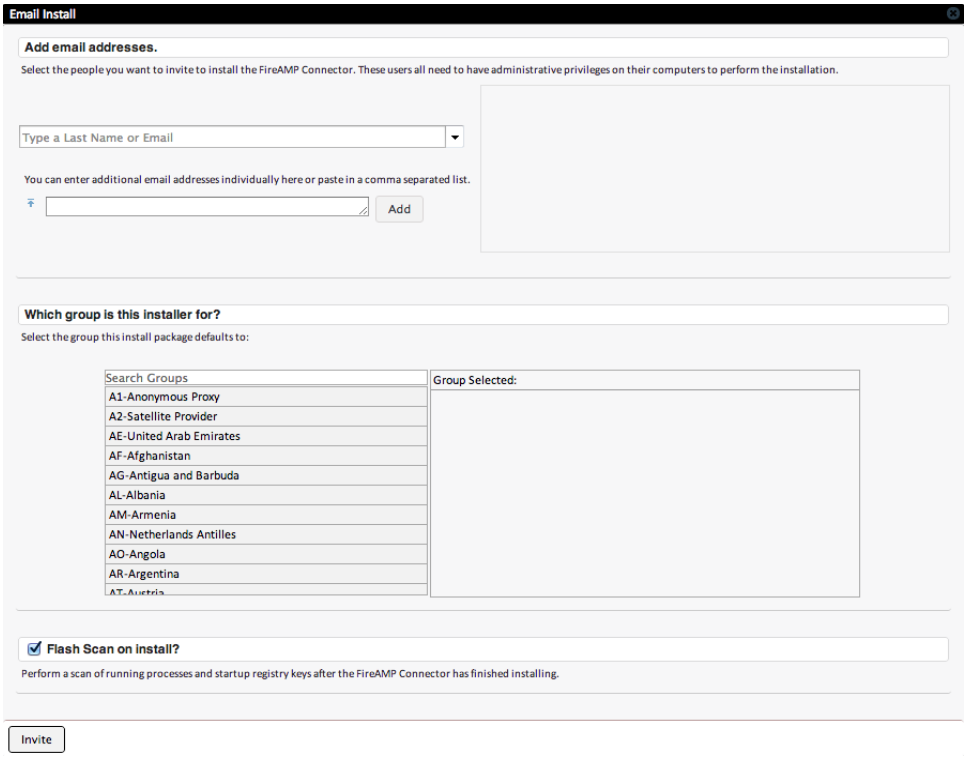


This screen also allows you to select the groups that the installer will be pushed to and whether or not a flash scan will be performed on install. The file name of the installer will include the name of the group you select. The flash scan checks processes currently running in memory and should be performed on each 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.

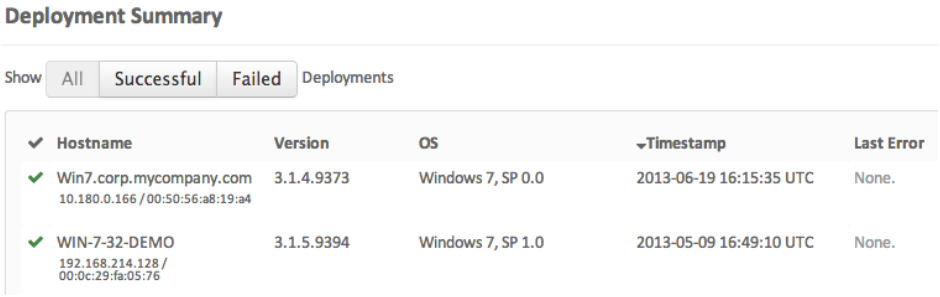
Email

The email install option allows you to send a link to the FireAMP Connector bootstrapper in an email to specified users. You can either choose the users at the top, manually enter email addresses you want to send the link to, or paste in a list of comma-separated email addresses. Like the direct download option you can select the group the installer is for so that they receive the appropriate policy.xml and choose whether or not to perform a flash scan on install. This deployment option is useful for remote users who do not connect to the network often but check their email regularly.



Deployment Summary

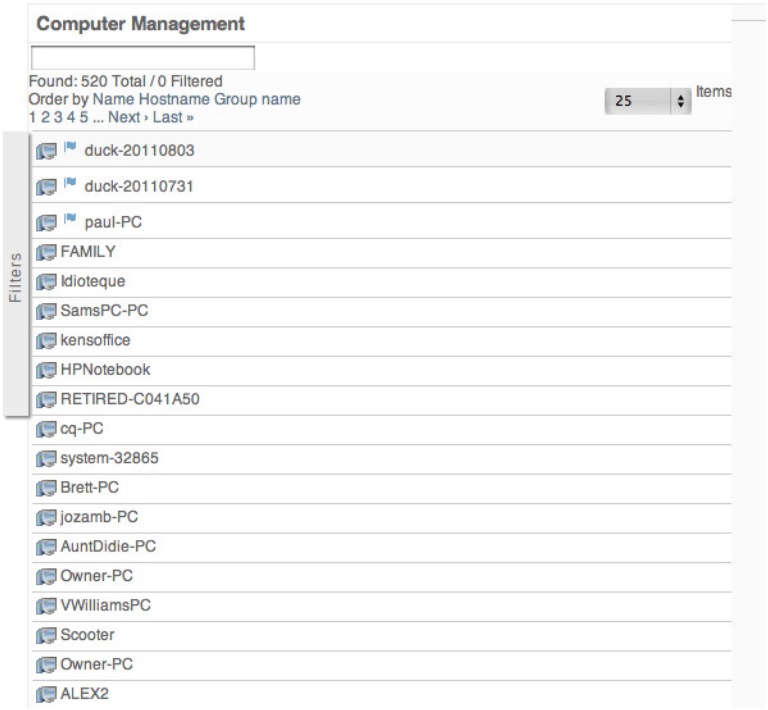
The Deployment Summary page gives you a list of the successful and failed FireAMP Connector installs.



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. You can apply filters to the list or navigate through the pages to view more computers.

Clicking on a computer in the list will expand details on that computer. From the detail you can change the Group the computer belongs to, see which Policy applies to it, along with other information about the computer. You can also run scans on the computer, delete it from the FireAMP organization, and flag or unflag the computer in the list. You can also click the **Browse events for this computer** button to open a filtered Events Tab view for the selected computer.

Chapter 7
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 Connector based on the operating system. The FireAMP Connector supports both 32-bit and 64-bit versions of these operating systems.

Microsoft Windows XP with Service Pack 3 or later

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

Microsoft Windows Vista with Service Pack 2 or later

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

Microsoft Windows 7

- 1 GHz or faster processor

- 1 GB RAM
- 150 MB available hard disk space - Cloud-only mode
- 1GB available hard disk space - TETRA

Microsoft Windows 8 and 8.1 requires FireAMP Connector 3.1.4 or later)

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

Microsoft Windows Server 2003

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

Microsoft Windows Server 2008

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

Incompatible software and configurations

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

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

The FireAMP 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 Connector to communicate withSourcefire systems, the firewall must allow the clients to connect to the following servers over HTTPS (TCP 443):

- Event Server - enterprise-event.amp.sourcefire.com
- Management Server - enterprise-mgmt.amp.sourcefire.com
- Policy Server - policy.amp.sourcefire.com.s3.amazonaws.com
- Error Reporting - crash.immunet.com

To allow the Connector to communicate with Sourcefire 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.sourcefire.com

In order to upload files for analysis, clients must be able to access the following server over TCP 80:

- Submission Server - submit.amp.sourcefire.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.immunet.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 sourcefire.com 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 sourcefire.com 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.

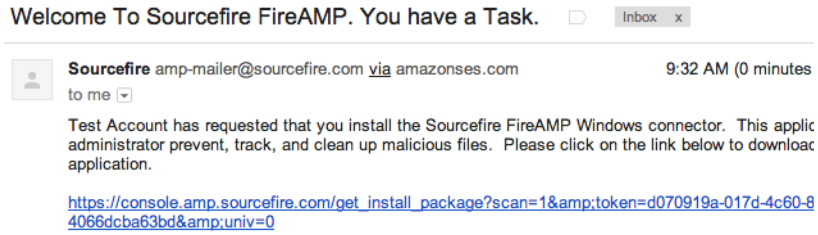
Installer

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

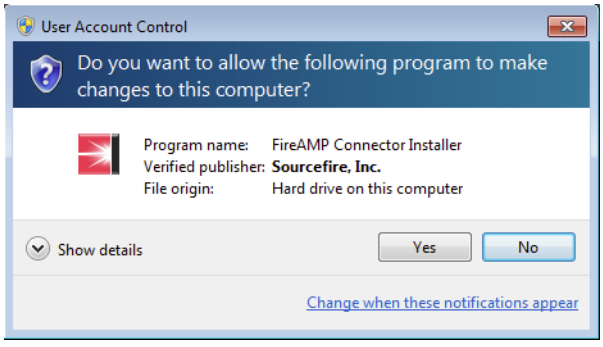
Interactive Installer

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.

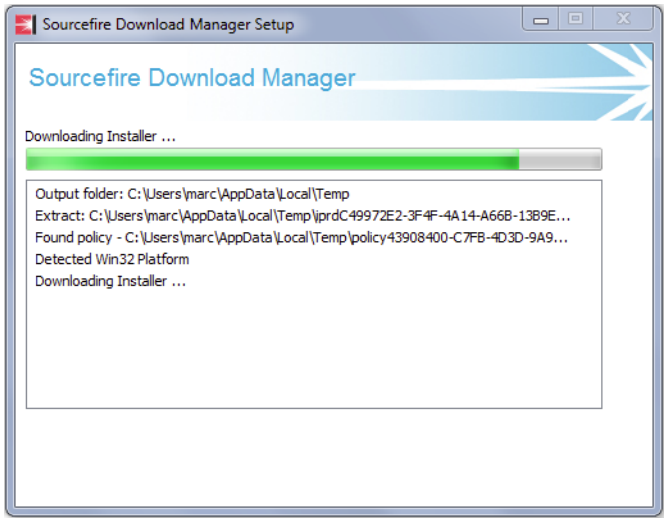
With the email method, the user will receive a message containing a link to the setup file. After the file has been downloaded, double-click on it to start the install.



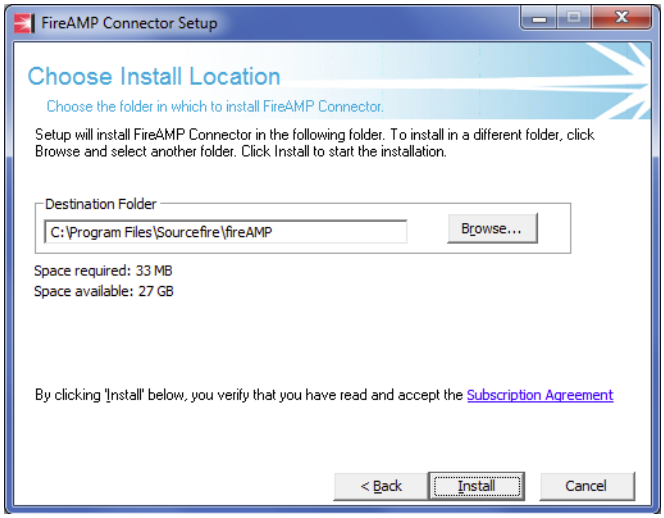
If Windows User Access Control (UAC) is enabled, the user will be presented with a prompt. Click on Yes to continue.



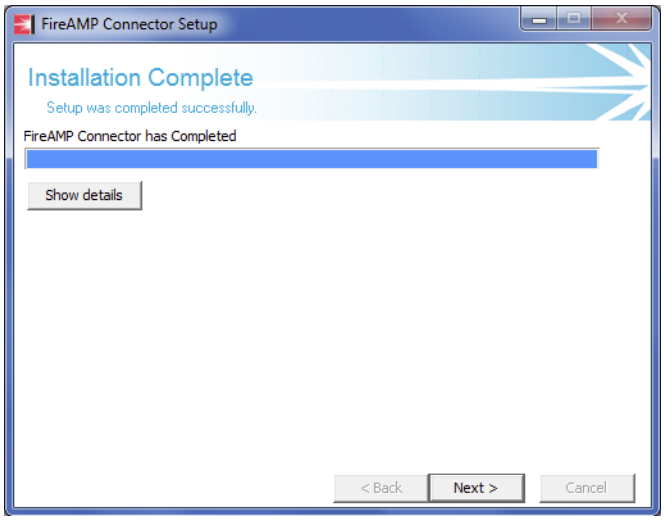
At this point the Download Manager will fetch the appropriate version of the installer package if installing through the bootstrapper. If the redistributable installer is used then this step will be skipped.



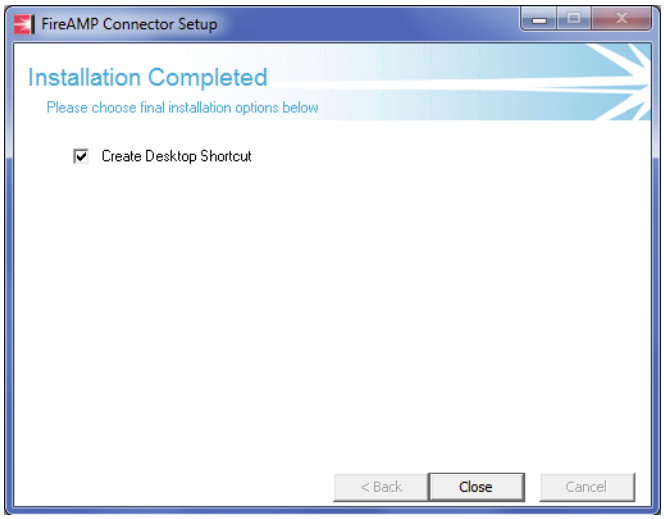
Next the user is presented with the install location dialog. In most cases the default location is the best choice. Links to the Connector End User License Agreement and Privacy Policy are also presented. Click Install to continue.



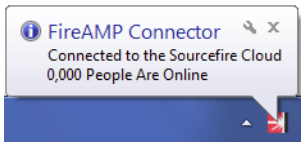
When the install is complete, click the Next button to continue.



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



If the option to run a Flash Scan on install was selected, that scan will now execute. The Windows System Tray icon will also indicate that you are now connected to the Sourcefire 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.
- /skipdfc 1 - Skip installation of the DFC driver.

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

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

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

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

  IMPORTANT! This must be specified as the last parameter.

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

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)

Connector User Interface

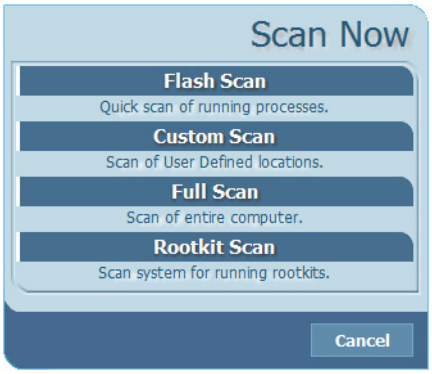
When the Connector is installed you can access it by double-clicking the desktop shortcut or clicking the FireAMP Connector entry in the Windows Start Menu.

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.

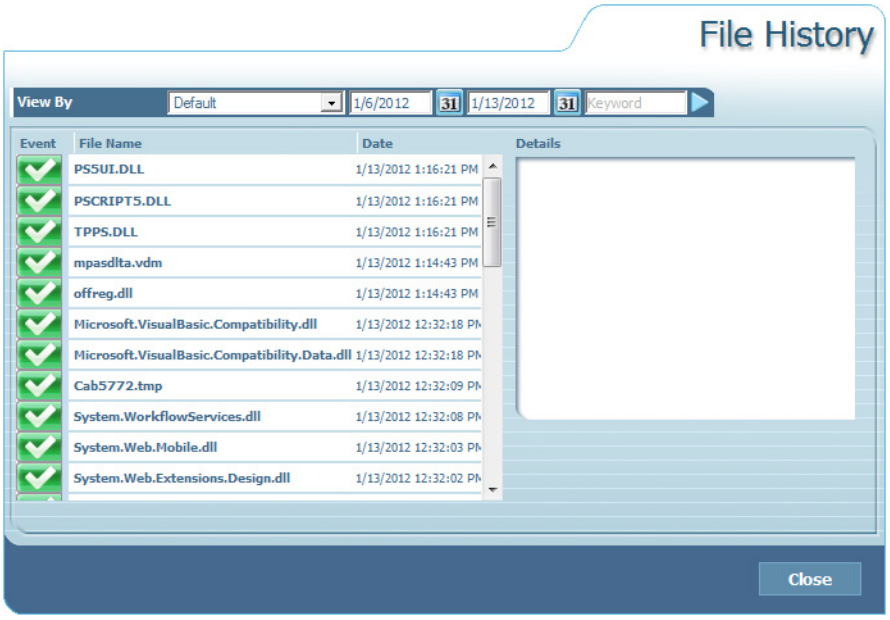
Custom Scan - Allows the user to define specific files or directories to scan. Selecting the Custom Scan will open a dialog allowing the user to specify what should be scanned.

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

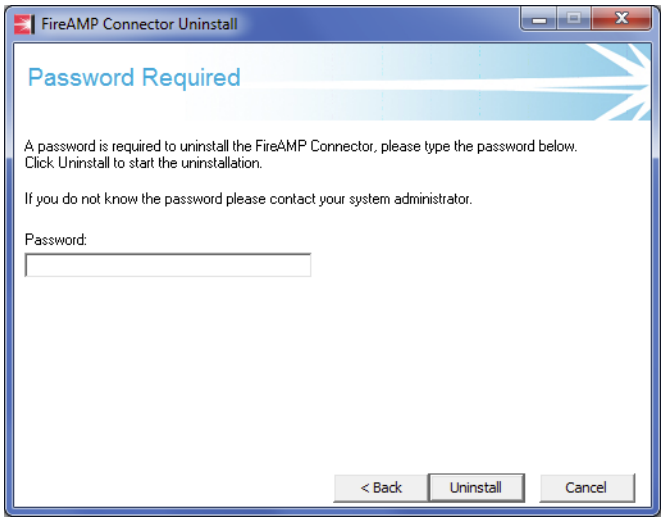
The Settings interface allows the individual user to see how the policy administrator has chosen to configure all aspects of the policy applied to the particular Connector. In a managed install all the entries in the settings are read-only and provided solely for informational and diagnostic purposes.

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.



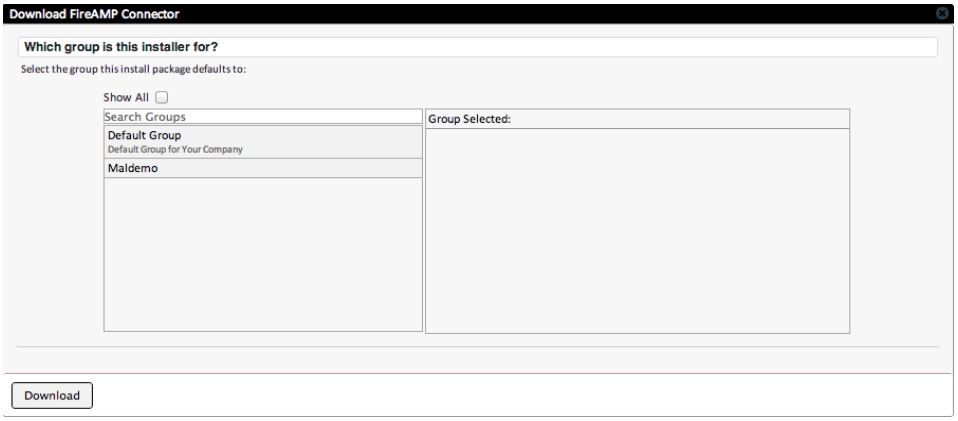
When the uninstall process finishes click the Close button. Finally, you will be presented with a prompt asking if you want to delete all the FireAMP Connector history and quarantine files. Reboot the computer to complete the uninstall process.

CHAPTER 8
DEPLOYING THE FIREAMP MOBILE CONNECTOR

The FireAMP Mobile Connector can be deployed by downloading the app or emailing a link to the app download to users. When the app is installed on a mobile device, an activation code will need to be entered.

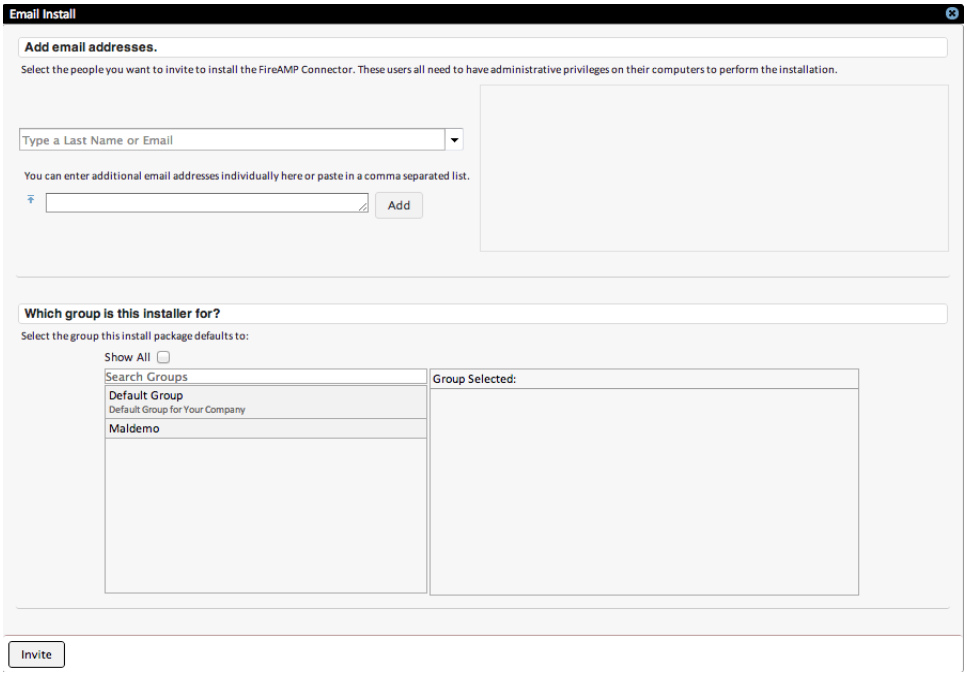
Download

The download option allows you to download the FireAMP Mobile Connector apk file for distribution to your devices. The file is approximately 2 MB in size and can be hosted in a location accessible to mobile devices in your organization. This screen also allows you to select the groups that the devices belong to.



Email

The email install option allows you to send a link to the FireAMP Mobile Connector apk in an email to specified users. You can either choose the users at the top, manually enter email addresses you want to send the link to, or paste in a list of comma-separated email addresses. Like the direct download option you can select the group the Connector is for so that they receive the appropriate policy.



Activation Codes

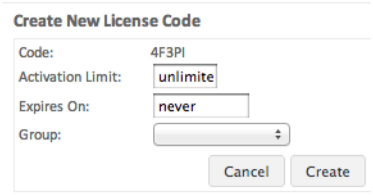
The Activation Codes screen allows you to generate activation codes required during FireAMP Mobile Connector installation on a device. To generate a new activation code click Create.

Select the limit for the number of activations that can be performed using this code by entering the value in the Activation Limit field. By default the value is set

to unlimited. Next choose the expiry date for the code using the calendar pulldown.

IMPORTANT! After the expiration date new FireAMP Mobile Connectors cannot be activated using the code but FireAMP Mobile Connectors that were activated using the code prior to the date will continue to function as normal.

Activation codes are set to never expire by default. Finally, select the Group the activation code will be used by. Only one activation code can be applied to a group at a time, so make sure you have assigned a high enough activation limit for the number of devices in the group you are applying the code to. Click Create to create the new activation code.



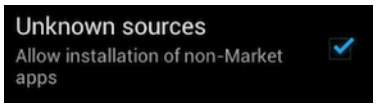
At any time you can change the settings for an activation code by clicking the Edit link next to its entry. You can also remove an activation code by clicking the Delete link next to its entry.

IMPORTANT! When you delete an activation code all FireAMP Mobile Connectors previously activated with that code will continue to function but new FireAMP Mobile Connectors can not be activated using that code.

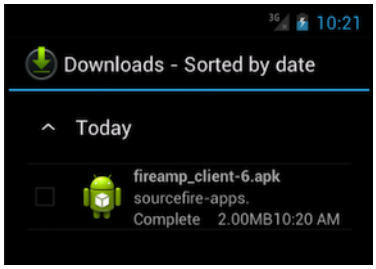
CHAPTER 9
FIREAMP MOBILE CONNECTOR

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

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



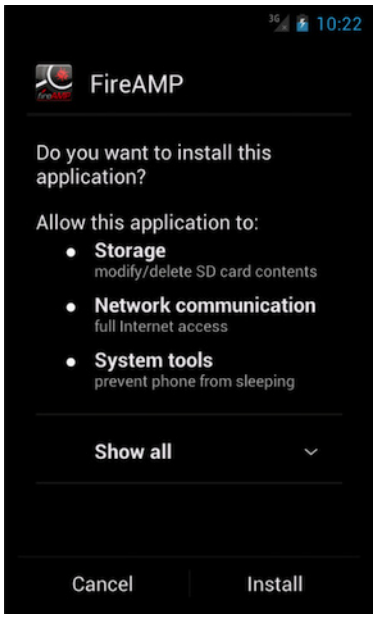
Once the fireamp_client.apk file has been downloaded it will be located in the device Downloads folder.



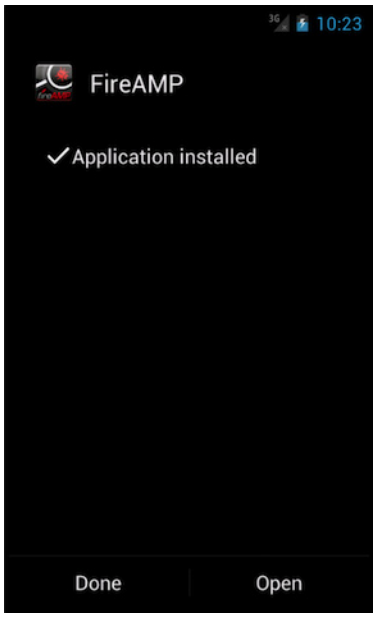
Simply tap the downloaded file to begin installation.

Installer

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

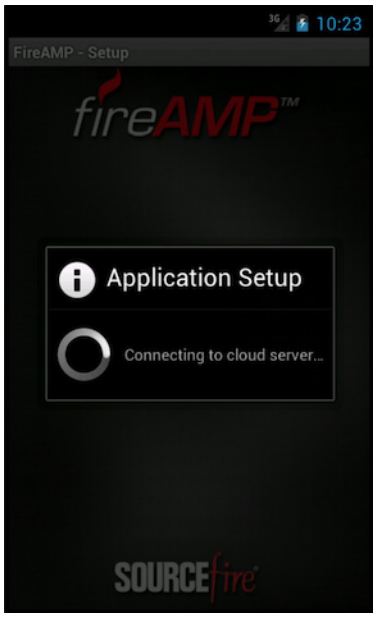


Once installation is complete, select Open to launch the application.

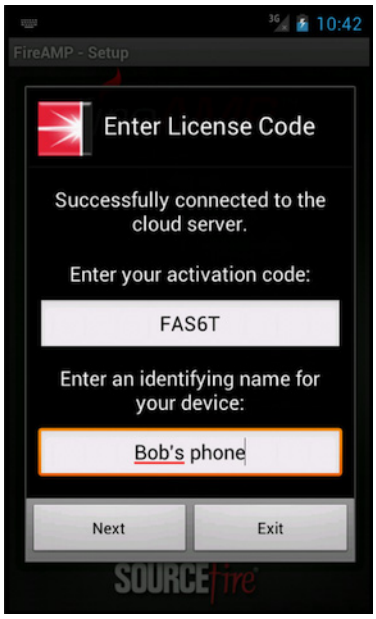


To agree to the license terms select Accept.

The FireAMP Mobile Connector will then attempt to establish a connection to the Sourcefire Cloud.



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



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

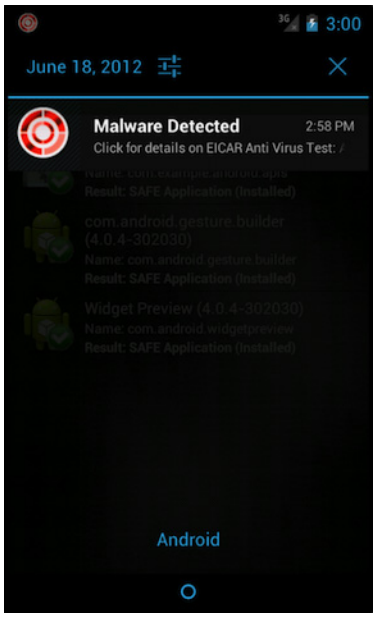
The application will begin an initial scan of the device for any malicious or non-compliant apps. If any are found either a yellow or red warning icon is displayed indicating that further action is required.

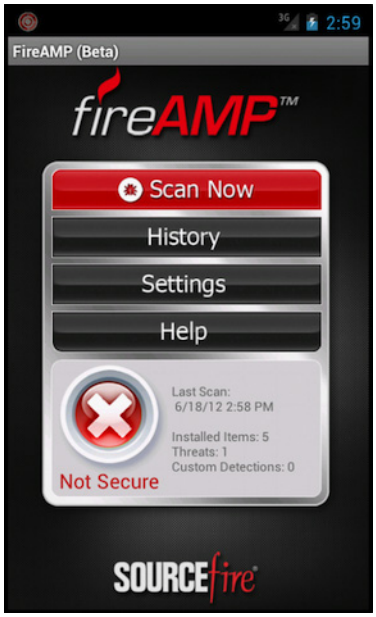
If no threats or non-compliant apps are detected a green check mark will indicate that the device is secure.

Removing Threats

If at any time a threat or non-compliant app is detected on the device, the user must take steps to remediate it.

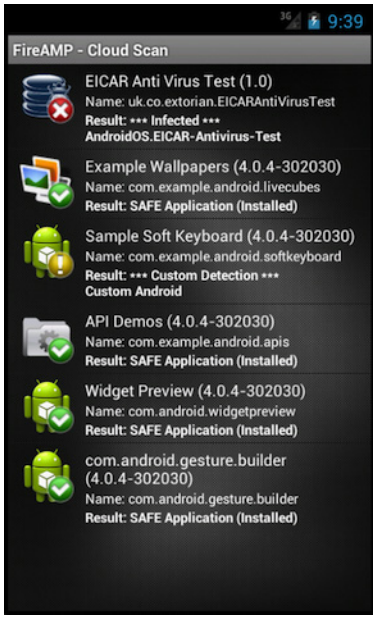
When a threat is detected a notification will appear in the status bar. Further information can be viewed by expanding the notification center or opening the FireAMP Mobile app.



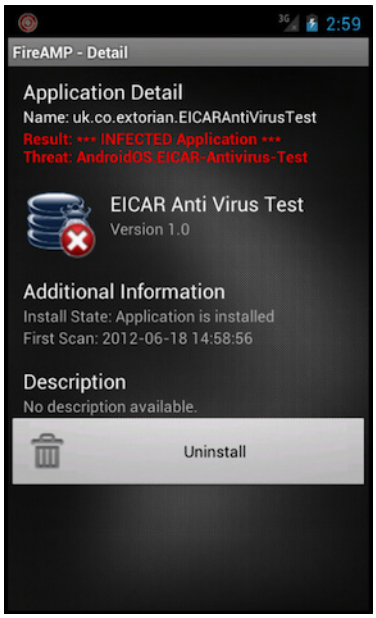


After a scan is completed a summary is displayed showing how many apps were scanned, how many of those apps were clean, the number that were malicious, and the number matching an entry in an Android Custom Detections list.

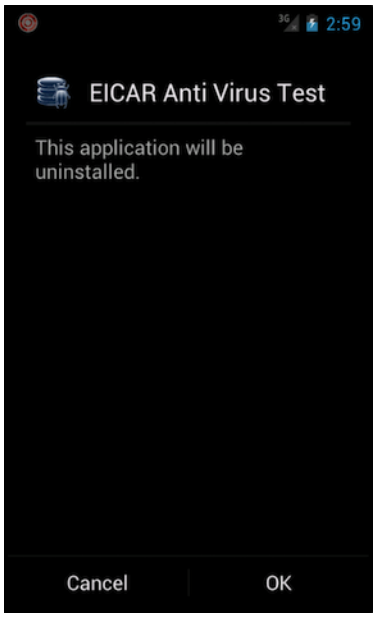
Next you can view the list of scanned applications on the device. Any malicious apps are indicated by a red warning icon along with the name of the detection while any custom detections are indicated by a yellow warning icon and the name of the custom detection list.



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



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

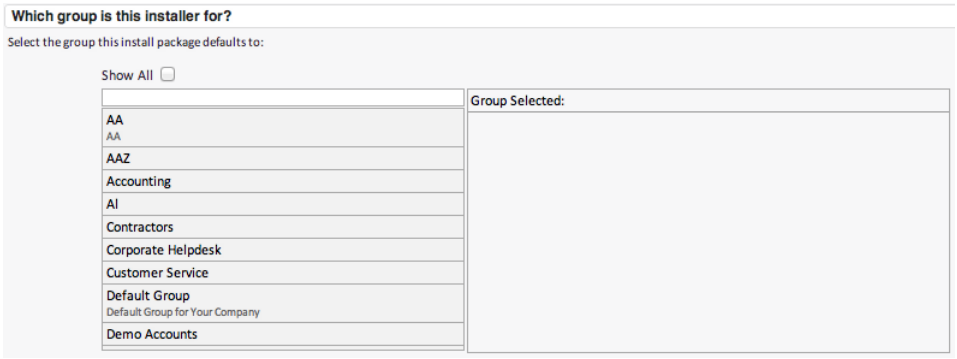


Chapter 10
Deploying the FireAMP Mac Connector

There are two ways to install the FireAMP Connector on client computers - direct download and email. This section will walk you through both.

Direct Download

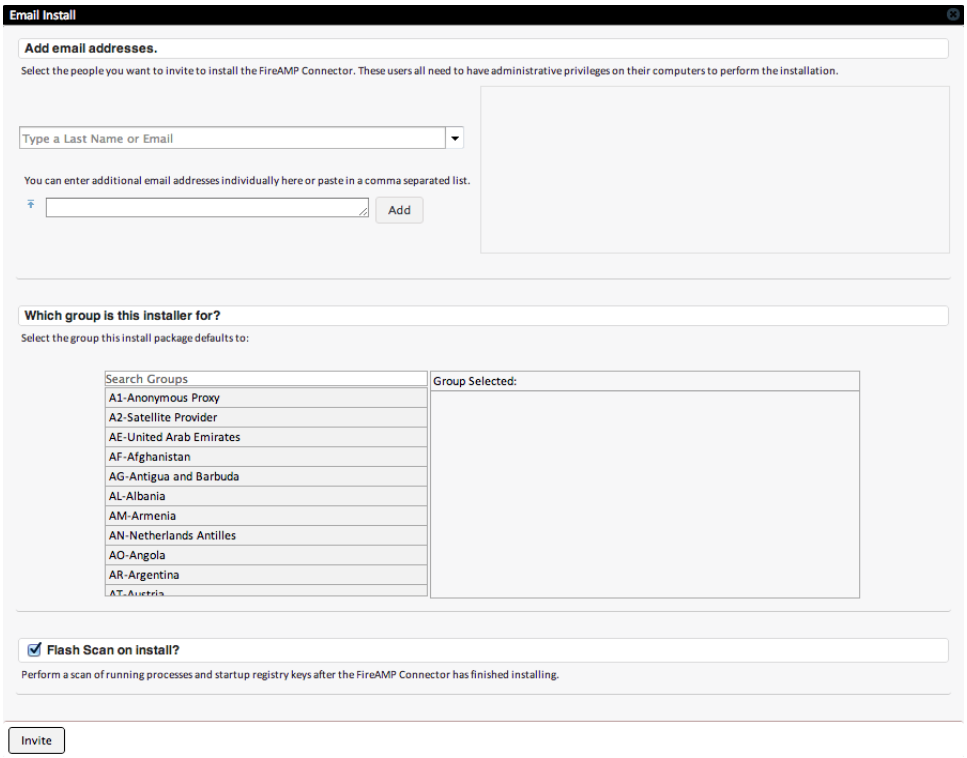
The direct download option allows you to download the pkg file to install the FireAMP Mac Connector. The installer is approximately 5 MB and can be placed on a network share.



This screen also allows you to select the groups that the installer will be pushed to and whether or not a flash scan will be performed on install. The file name of the installer will include the name of the group you select. The flash scan checks processes currently running in memory and should be performed on each install.

Email

The email install option allows you to send a link to the FireAMP Mac Connector in an email to specified users. You can either choose the users at the top, manually enter email addresses you want to send the link to, or paste in a list of comma-separated email addresses. Like the direct download option you can select the group the installer is for so that they receive the appropriate policy.xml and choose whether or not to perform a flash scan on install. This deployment option is useful for remote users who do not connect to the network often but check their email regularly.



Chapter 11
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 FireAMP Mac Connector can be installed on 64-bit Macs running OS X 10.7 to 10.9 with approximately 65 MB of free disk space.

Incompatible Software and Configurations

The FireAMP 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 Connector to communicate withSourcefire systems, the firewall must allow the clients to connect to the following servers over HTTPS (TCP 443):

- Event Server - enterprise-event.amp.sourcefire.com
- Management Server - enterprise-mgmt.amp.sourcefire.com
- Policy Server - policy.amp.sourcefire.com.s3.amazonaws.com
- Error Reporting - crash.immunet.com

To allow the Connector to communicate with Sourcefire 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.sourcefire.com

In order to upload files for analysis, clients must be able to access the following server over TCP 80:

- Submission Server - submit.amp.sourcefire.com

Installing the FireAMP Mac Connector

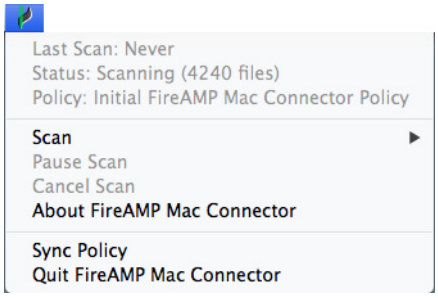
The FireAMP Mac Connector does not use a signed installer package so rather than simply double-clicking on the pkg file, you have to right-click the pkg file and select Open. When prompted that the file is from an unidentified developer click Open and you will be presented with the initial installer screen. Click Continue to proceed.

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

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

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.

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`

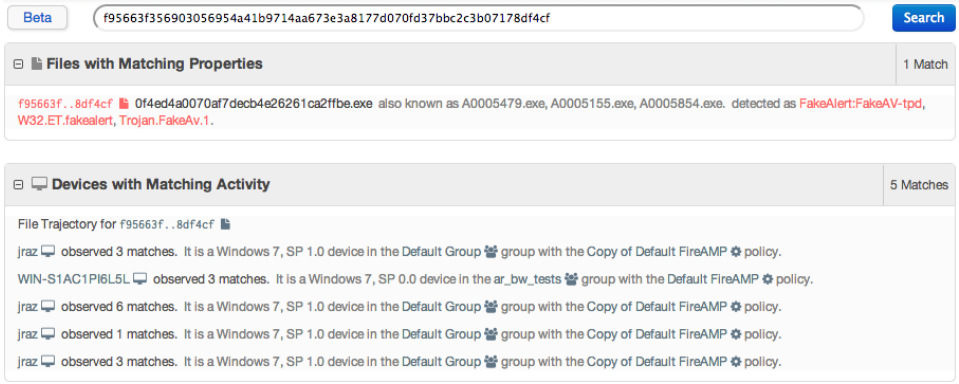
CHAPTER 12
SEARCH

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.

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

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

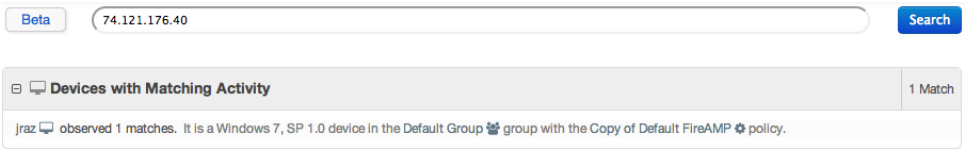
Enter an exact email address or user name to find any matching users in your FireAMP deployment.

Network Activity Searches

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

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

Host name and URL searches can be 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.



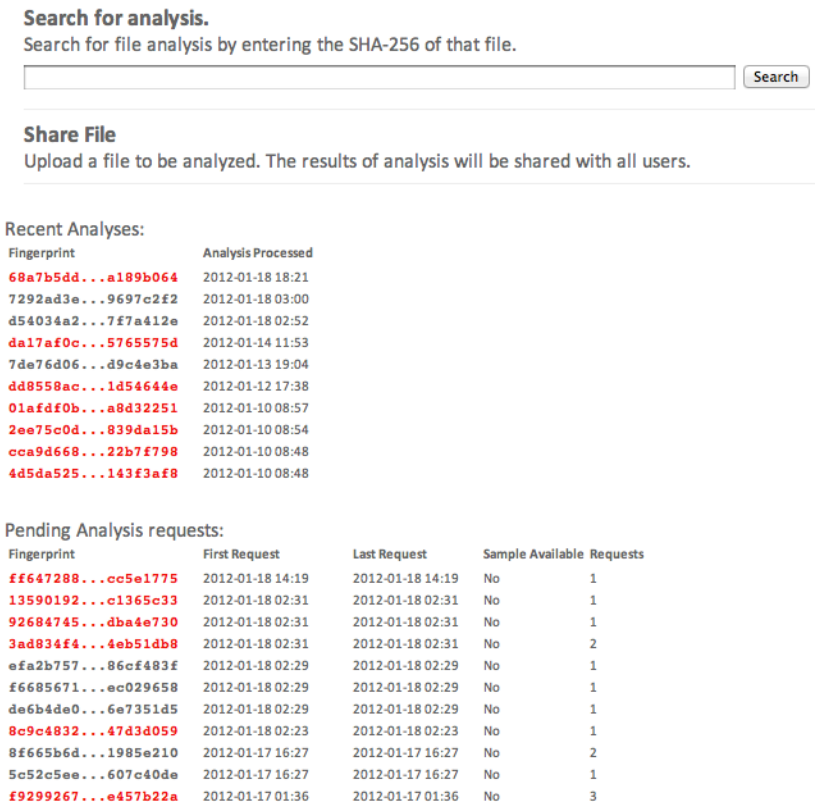
CHAPTER 13
FILE ANALYSIS

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 results are then made available to all FireAMP users. 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 Joe Security LLC.

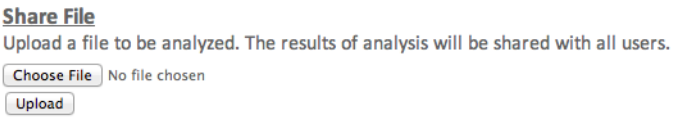
To navigate to the File Analysis page click on **Analysis > File Analysis**.

File Analysis Landing Page

When you navigate to the File Analysis landing page click on the links to Recent Analyses that have already completed or view the Pending Analysis requests.



You can also paste the SHA-256 of the file you want to view an analysis for into the Search for analysis field. If an analysis exists for this SHA-256 it will be rendered in the browser.



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 and shared with the community. To do this, click Choose File, select the file you want to upload, 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.

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 supports the following applications:

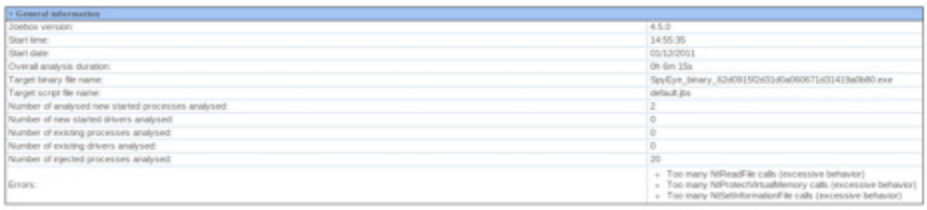
- Adobe Reader 9.1
- Adobe Flash 10.3r181
- Microsoft Office Professional Plus 2010

This means that any files supported by these applications as well as Microsoft Windows executable files can be analyzed. If you require additional application support in the File Analysis sandbox, please email support@sourcefire.com.

WARNING! When uploading a file for analysis it will be available to all other FireAMP users. Exercise judgment before uploading a file that may contain sensitive information.

General Information

When you browse to an analysis it has the following format.



The General Information section contains information about the sandbox instance that executed the file.

Classification / Threat Score

When available the Classification/Threat Score section contains a series of ratings for the maliciousness of the analyzed binary. Green is benign, red is malicious. The ratings are determined heuristically and have the following categories:

- Persistence, Installation Boot Survival
- Hiding, Stealthiness, Detection and Removal Protection
- Security Solution/Mechanism bypass, termination and removal, Anti Debugging, VM Detection
- Spreading
- Exploiting
- Networking

- Data spying, Sniffing, Keylogging, Ebanking Fraud

This section can be used to quickly determine if an executable is relatively benign, suspicious, or highly malicious. You can then use this high-level information to triage security incidents.

Signature Detection

The Signature Detection section is similar to the Classification/Thread Score section in that it contains executable behaviors that were observed in the analyzed binary. The behaviors are stack-ranked and color-coded. Blue is a relatively benign behavior and red is usually malicious.

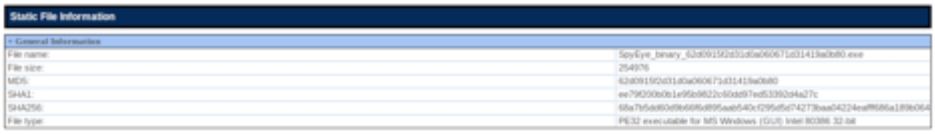
This information can be quickly used to determine if an executable is relatively benign, suspicious, or malicious. You can then use this high level information to triage security incidents, or to direct further analysis of the executable.

Static File Information

The Static File Information section of the analysis has information about the file that was uploaded, prior to execution. This information is gleaned by parsing the file on disk.

General Information

This section contains the file name, size, MD5, SHA1, SHA-256, and file type of the uploaded file. This information can be used to search other intelligence sources for details on this file.



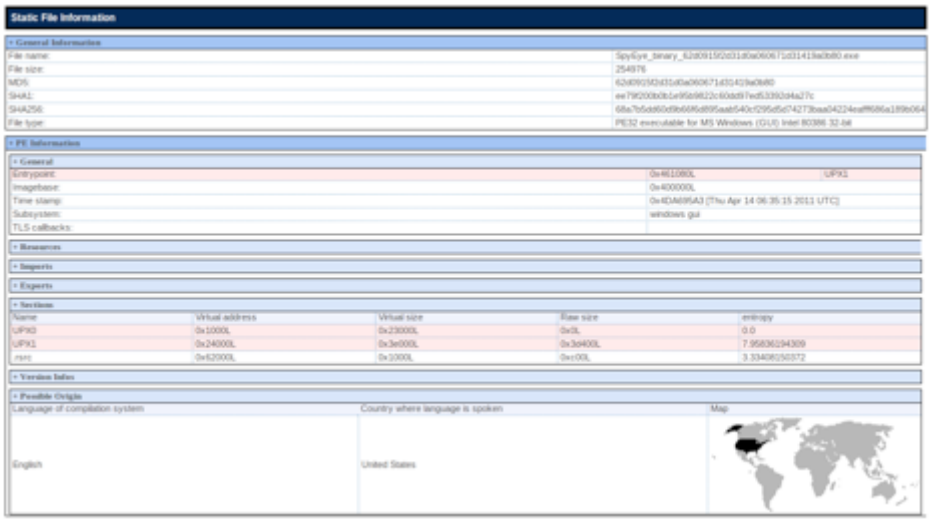
PE Information

The PE Information subsection is divided into several additional sections that describe the portable executable file. These sections (when available) are:

- General
- Resources
- Imports
- Exports
- Sections
- Version Infos
- Possible Origin

This information can be used to get a quick understanding of the properties of the application. For example, the Entrypoint field in the General section can be used to determine if the file is packed. In the screenshot, the entry point is in the UPX1 section; this section is non-standard in portable executable files. This means that this file is most likely packed using the UPX packer. The Resources, Imports, and Exports can sometimes give the analyst a general understanding of what the executable does however, all of these sections can be destroyed and/or

obfuscated if the file is packed leaving only the Resources, Imports, and Exports of the packer exposed until the file is unpacked or executed.



The Version Info and Possible Origin can sometimes be used to tell when the file was compiled and on what language version of operating system the file was compiled. This can be useful to give hints to the analyst about the origin of the attack. It should be noted though, that a good deal of information in this section can be obfuscated or spoofed. Great care needs to be taken when using this information without further analysis.

String Analysis

The String Analysis section contains lists of human-readable strings that were extracted while analyzing the binary. These strings can be used to give clues about the executable behavior, as well the strings can be URLs of websites, IRC commands, or other useful data that can be used for IDS signatures to prevent the malicious code communicating with controllers.

Formattings for printf style functions

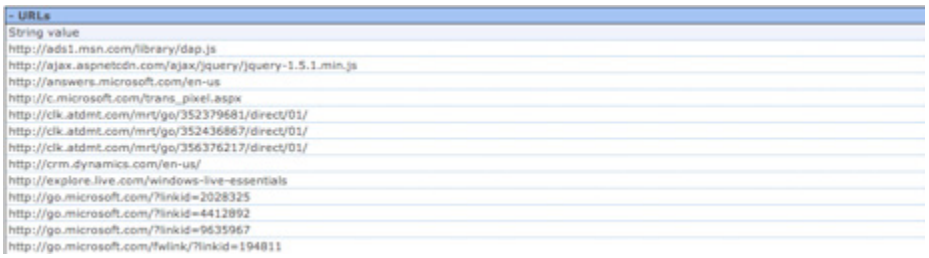
When available, the Formattings for printf style functions subsection contains a list of strings that have been extracted from the executable. The strings in this section can be used to create rudimentary Snort IDS and FireAMP signatures that can be used as a rapid measure to control an incoming infection. The signature

can be made more sophisticated later. Strings in a binary can sometimes give a security professional a quick overview of some of the behaviors of the threat.

- Formattings for printf style functions	
String value	Source
[ERROR] : dwErr == %u (Could be invalid encryption key)	B6232F3AC2C.exe, SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe
! R]\%C	B6232F3AC2C.exe.dr
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\%d	B6232F3AC2C.exe, SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe
r = %s	B6232F3AC2C.exe, SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe
threadmetadataInfo%d	SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe
[ERROR] : dwErr == %u	B6232F3AC2C.exe, SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe
[ERROR] : dwErr == %u (Config is damaged)	B6232F3AC2C.exe, SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe
%s\Content.IE5\%s	B6232F3AC2C.exe, SpyEye_binary_62d0915f2d31d0a060671d31419a0b80.exe

URLs

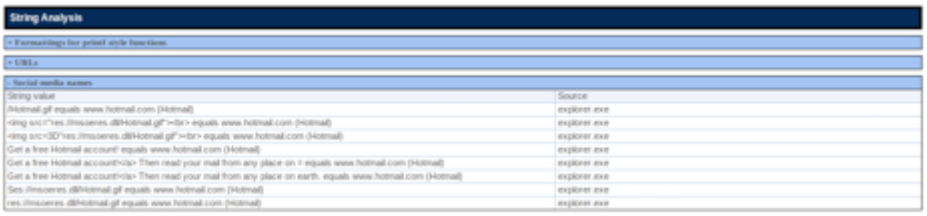
When available, the URLs subsection will display URLs that were found while analyzing the file. These can be URLs that the sample contacts, redirects, or simply monitors.



- URLs
String value
http://ads1.msn.com/library/dap.js
http://ajax.aspnetcdn.com/ajax/jquery/jquery-1.5.1.min.js
http://answers.microsoft.com/en-us
http://c.microsoft.com/trans_pixel.aspx
http://clk.atdmt.com/mrt/go/352379681/direct/01/
http://clk.atdmt.com/mrt/go/352436867/direct/01/
http://clk.atdmt.com/mrt/go/356376217/direct/01/
http://crm.dynamics.com/en-us/
http://explore.live.com/windows-live-essentials
http://go.microsoft.com/?linkid=2028325
http://go.microsoft.com/?linkid=4412892
http://go.microsoft.com/?linkid=9635967
http://go.microsoft.com/fwlink/?linkid=194811

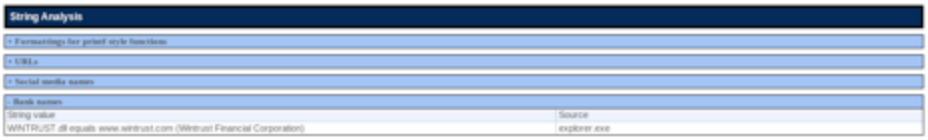
Social Media Names

When available, the Social media names subsection will display strings that correlate to common social media websites. These might be included for various purposes like account hijacking or for propagation.



Bank Names

When available, the Bank names subsection displays strings that correlate to popular financial institutions. These strings are frequently seen in malware that attempts to steal online banking credentials or hijack sessions.



Analysis Overview

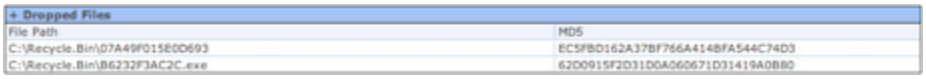
The Analysis Overview is comprised of several sections Startup, Dropped Files, and Involved IP Addresses.

Startup

The Startup section contains a list of files that execute in the sandbox during startup, the cleanup section is the files that execute on shutdown.

Dropped Files

These are the files that were dropped (created by the sample under analysis) in the sandbox while the file was being analyzed.



Involved IP Addresses

These are the IP addresses that were involved during analysis. They might be command and control servers in the case of a bot, sites containing additional malware the sample attempts to download, or other involved sites.

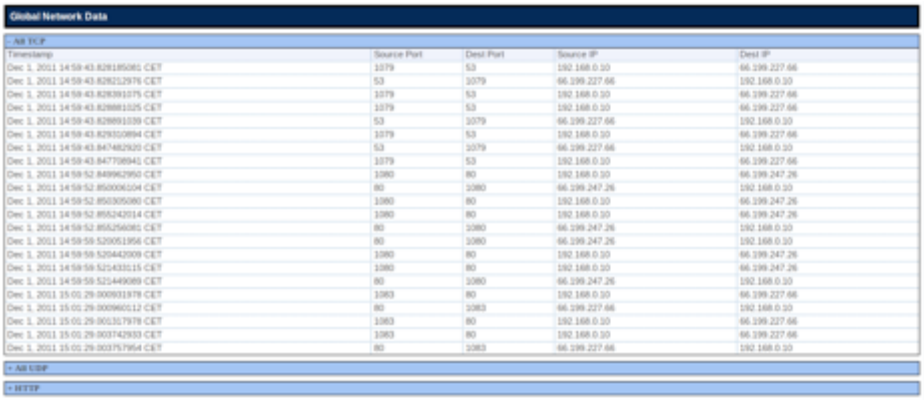
+ Involved IP Addresses			
IP	ASN	ASN Description	ANS State
66.199.227.66	AS15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US
66.199.247.26	AS15149	EZZI-101-BGP - Access Integrated Technologies, Inc.	US
195.186.1.121	AS44038	BLUEWIN-AS Swisscom (Schweiz) AG	CH

Global Network Data

The Global Network Data section contains a summary of all of the interesting network traffic that was generated while analyzing the file. This section has the following subsections (when available):

- All TCP
- All UDP
- HTTP
- DNS Query
- DNS Answer
- IRC

All TCP and All UDP are summaries of all of the TCP/UDP traffic observed while analyzing this file. The IP address and port information here can be used to create rudimentary rules on a firewall to restrict ingress/egress activity to certain ports and IP addresses that are known to be associated with malicious code.



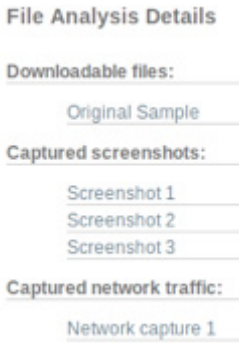
DNS Query and DNS Answer are lists of DNS transactions that were observed while analyzing the file. These queries can be used to detect hosts that are

infected on your network, or as a guideline on what domain names need to be sinkholed or blocked in order to control an infection on your network.

HTTP and IRC subsections contain HTTP and IRC traffic that was observed while analyzing the executable. This information can be used to write network IDS signatures or to block ingress/egress communications with these hosts at the network perimeter in order to prevent further control of infected hosts.

File Analysis Details

The File Analysis Details section allows you to download the original sample (executable) that was executed in the sandbox. This is very useful if you want to perform a deep analysis on the executable and it can also be used to create Simple Custom Detections and Advanced Custom Signatures to control and remove breakouts in a network.



You can also download the entire network capture that was collected while analyzing the binary. 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.

When analyzing malware a series of screenshots are also collected. These screenshots can be used to observe the visual impact that the malware has on the desktop of a victim. The screenshots 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.

CHAPTER 14
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:

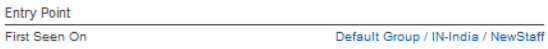
- Clean files – 7 days
- Unknown files – 1 hour
- Malicious files – 1 hour

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

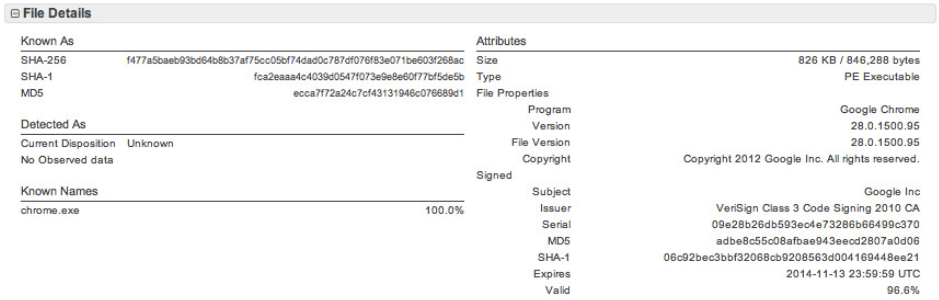
Visibility – includes the First Seen and Last Seen dates and the total number of Observations of the file in question in your network. Observations shows the number of times that the file in question was both a source of activity and when it was a target of activity. Note that the number of Observations 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.



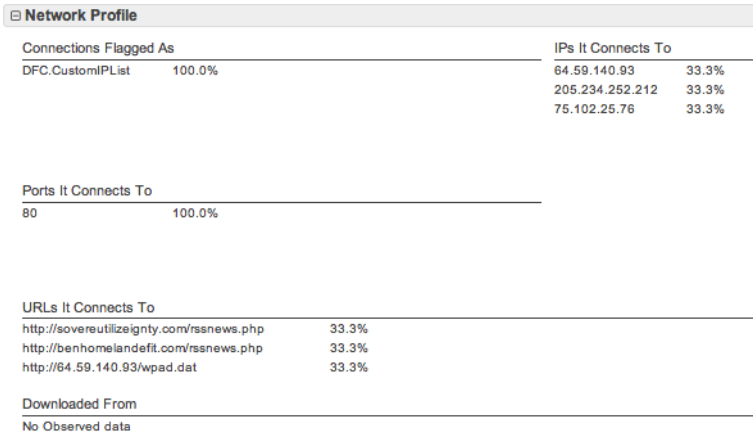
Created By – identifies the files that created the threat in question by their SHA-256. This includes the number of times the threat was created by that file in both your network and among all FireAMP users. Where available the file name and product information are also included. It is important to note 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.



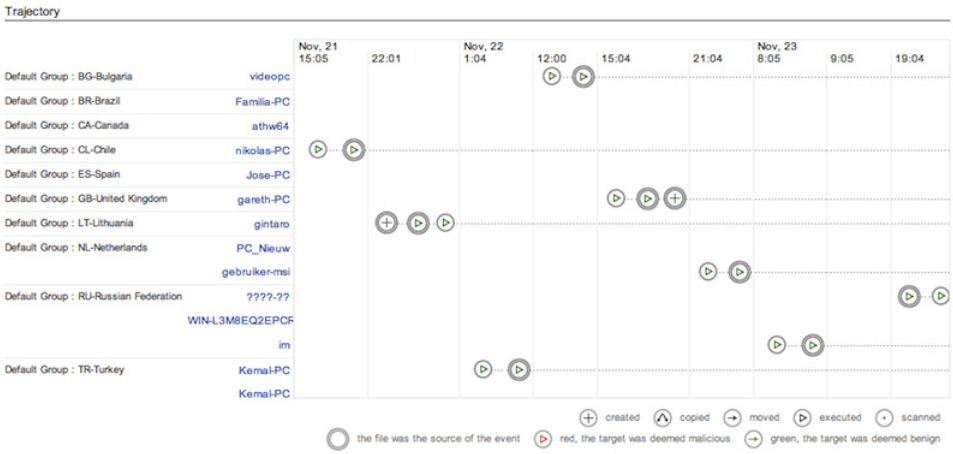
- Known As shows the SHA-256, SHA-1, and MD5 hash of the file.
- Attributes displays the file size and type.
- Known Names includes any names the file went by on your network.
- Detected As shows any detection names in the case of a malicious file.

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

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

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

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

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

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


Event History

date	computer	group	event	sha256	filename	product	disposition
Mar 21, 0:30:16	HR-130	Demo Accounts : HR	Created by	f9232b...d32189	*explorer.exe*	Microsoft® Windows® Operating System 6.0.2900.3264	Detected as W32.SHEATH.COHORS.NOV.E83A61
Mar 21, 0:30:22	HR-130	Demo Accounts : HR	Executed by	f9232b...d32189	*explorer.exe*	Microsoft® Windows® Operating System 6.0.2900.3264	Detected as W32.SHEATH.COHORS.NOV.E83A61
Mar 21, 1:22:11	HR-130	Demo Accounts : HR	Created by	f9232b...d32189	*explorer.exe*	Microsoft® Windows® Operating System 6.0.2900.3264	Detected as W32.SHEATH.COHORS.NOV.E83A61
Mar 21, 1:42:17	HR-130	Demo Accounts : HR	Executed by	f9232b...d32189	*explorer.exe*	Microsoft® Windows® Operating System 6.0.2900.3264	Detected as W32.SHEATH.COHORS.NOV.E83A61

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 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:

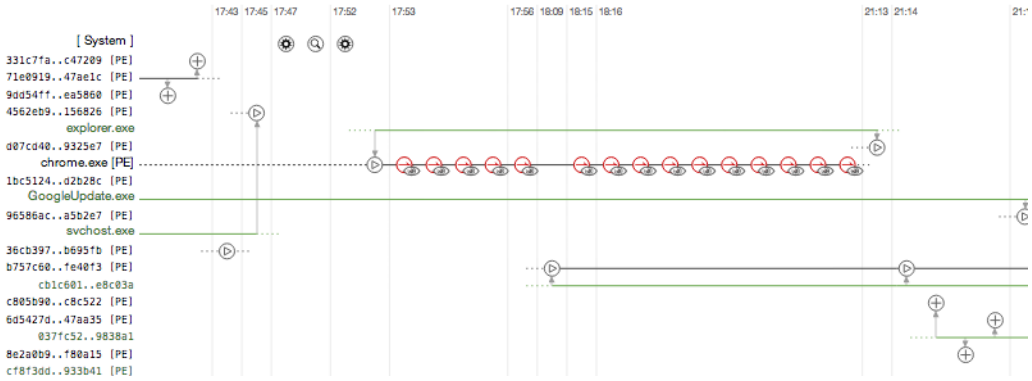
- Clean files – 7 days
- Unknown files – 1 hour
- Malicious files – 1 hour

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

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.

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.

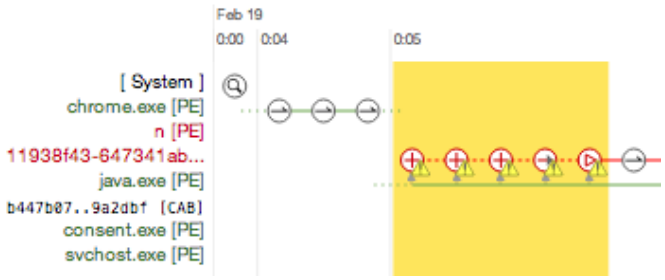
FireAMP Connector events are displayed next to the [System] label in Device Trajectory. Connector events include reboots, user-initiated scans and scheduled scans, policy and definition updates, Connector updates, and a Connector uninstall.

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:

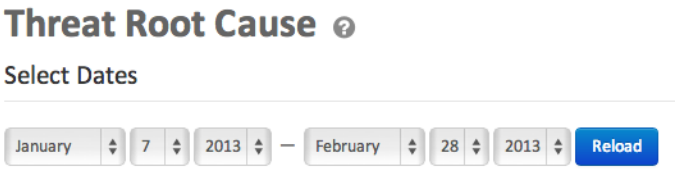
- Detection name
- SHA-256
- SHA-1
- MD5
- File name
- Directory name
- Local and remote IP addresses
- Port numbers
- URLs

CHAPTER 15
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

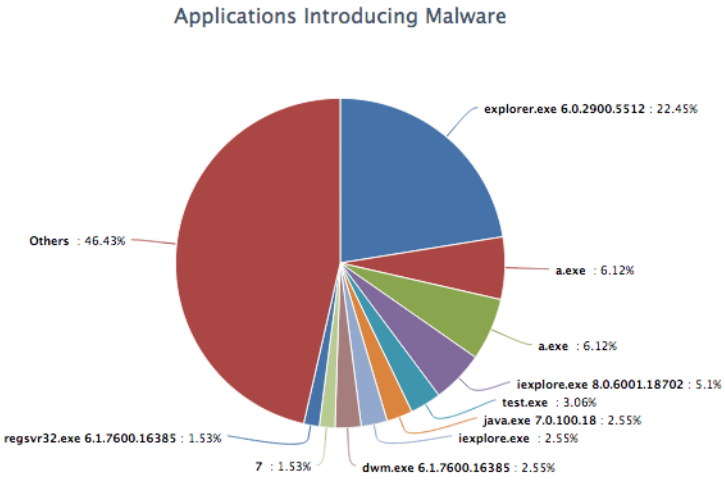
Threat Root Cause allows you to select a date range to view. By default the date range is set to show the previous day and current day. Select the start and end dates you want to view then click **Reload** to view the Threat Root Cause for the specified date range.



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.

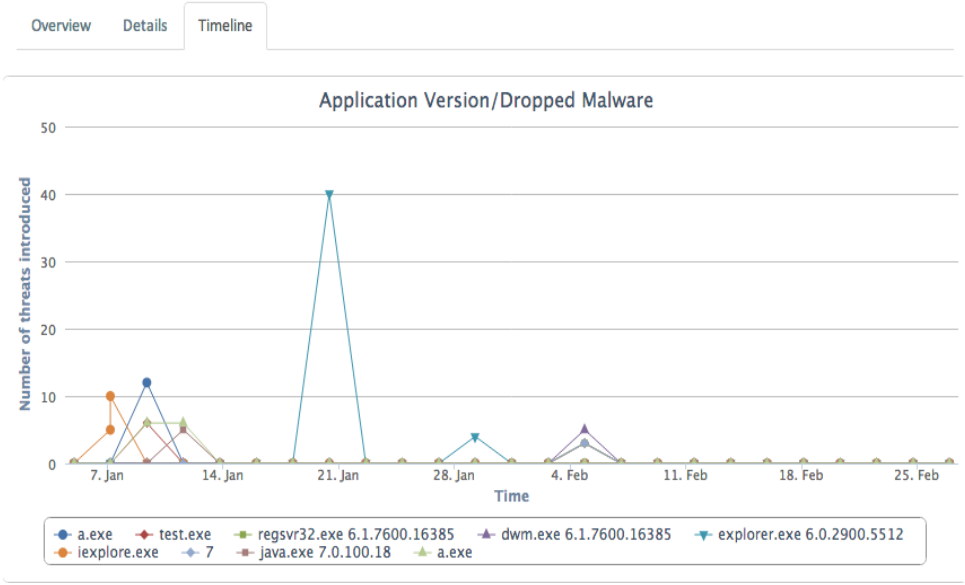
Program	Threat Name	Version	Threats Introduced	Computers Affected	Event Type
explorer.exe		6.0.2900.5512	44	3	44 moved
a.exe			12	2	4 created 4 executed 4 moved
a.exe			12	3	4 created 4 executed 4 moved
iexplore.exe		8.0.6001.18702	10	5	8 created 2 executed
test.exe			6	1	4 created 2 executed
java.exe		7.0.100.18	5	1	3 created 1 executed 1 moved
iexplore.exe			5	2	4 created 1 executed
dwm.exe		6.1.7600.16385	5	1	3 created 2 executed
7			3	1	2 created 1 executed
regsvr32.exe		6.1.7600.16385	3	1	2 created 1 executed

Clicking on the Program name in this view will take you to the Dasboard Events Tab with the view filtered to show all events where the particular program was the parent.

Timeline

The Timeline tab shows the frequency of malware downloaded into your environment by each application over the previous day. If one application is seen introducing many malware samples at once or consistently over the period it can indicate that the application is nothing more than a downloader for malware.

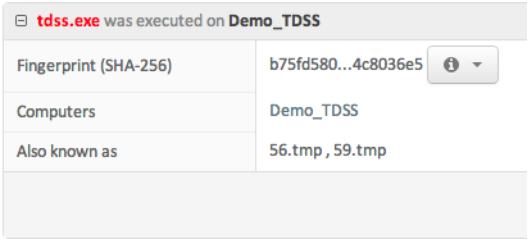
There is also a possibility that a vulnerable application being exploited to install malware could display similar behavior.



CHAPTER 16
PREVALENCE

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.

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. If more than one

computer executed the file, click on the name of the computer to view its Device Trajectory.

CHAPTER 17
REPORTING

Reports are a powerful feature of the FireAMP administration portal. They allow a user to view aggregate data generated from their environment for the past day, week, or month and can be run on demand or scheduled. They can be accessed by clicking on **Reports** on the main menu.

Creating a Report

To create a new report click on Create Report from the Reports screen. This will start the Report wizard to guide you through the steps required to create a report.

Select Data to Add

The first step to create a report is to choose the report type. The available reports are:

High Risk Computers - Designed to surface computers in your environment that are at high risk of compromise. The computers presented here might need more immediate attention than other computers deemed to be at a lower risk of exposure to malware.

Security Health - A broad presentation of the security posture of the set of selected computers under review.

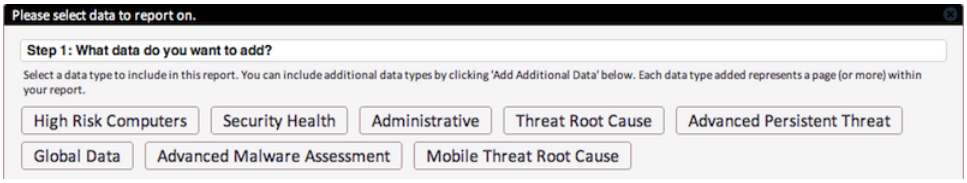
Administrative - Contains data detailing administrative issues for computer health and deployment as well as general information on the Groups that are configured for your environment.

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. The process name, software title, and version number (as stamped in the binary) of the implicated software are shown.

Advanced Persistent Threat - An Advanced Persistent Threat (APT) is a specialized form of malware attack. They are not accidentally picked up like conventional malware, but are created and launched by parties who are interested in targeting a specific network for attack. APTs appear to be unique globally but are found only on the targeted network, making them difficult to detect. This list describes a set of potential APTs on your network. A piece of malware cannot be definitively diagnosed as an APT without further analysis.

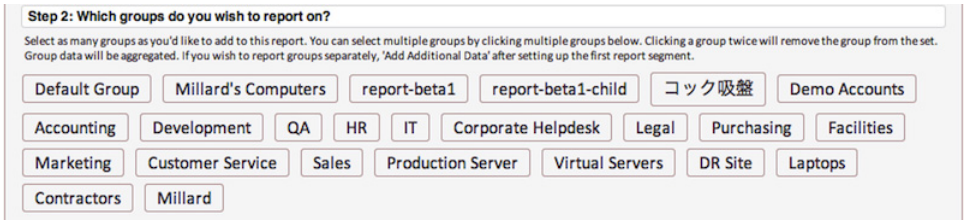
Advanced Malware Assessment - This report provides a summary of your organization's overall security posture and exposure to advanced malware as a result of the deep visibility and extensive control capabilities in FireAMP.

Mobile Threat Root Cause - This report is only available if you have a FireAMP Mobile license. It provides information on apps introducing malware on your mobile devices as well as the top malware detected on your devices, the top offenders, and the top policy violators.



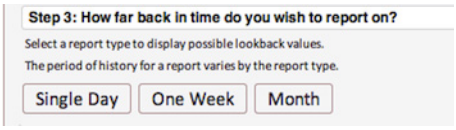
Select Groups

After you have selected the type of report you want, select the groups you want to include in the report. Multiple groups can be selected, however, the data for the groups will be aggregated. If you want to view the same data for each group separately in the same report you can add additional data.



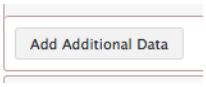
Select Reporting Range

Next, select the reporting period you want to view. You can select a single day, one week, or one month.



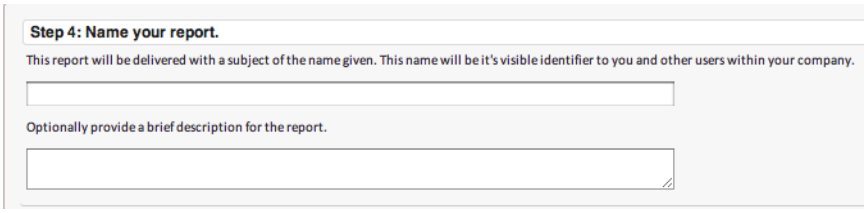
Add Additional Data

In some cases you might want to include multiple data sets in a single report. To do this, click the Add Additional Data button and repeat the above steps. You can continue doing this until you have added all the data sets you want to include in the report.



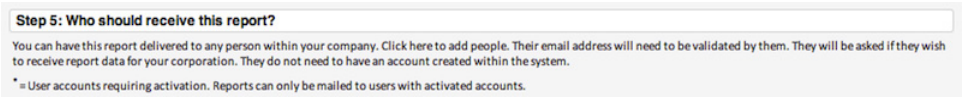
Name the Report

Provide a name and optionally a brief description for the report. Giving the report a meaningful name is important because you might want to run it again at a later date. The report will also remain in your report history for future reference.



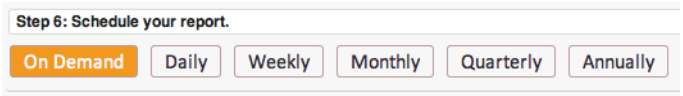
Select Recipients

Select one or more recipients for the report. You can also use the Click here to add people link to send the report to one or more email addresses that do not have FireAMP accounts.



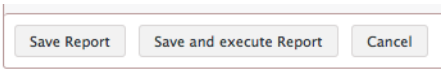
Schedule the Report

Choose when you want the report to run. On Demand means that the report will only be generated when it is manually invoked.



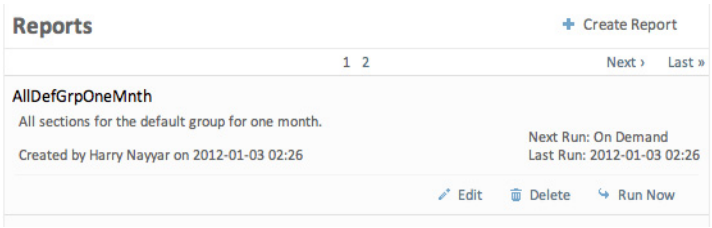
Save and Execute the Report

After you are satisfied with all your report options you can save the report settings to execute at a later date, save the settings and execute the report immediately, or cancel the report without saving the settings.



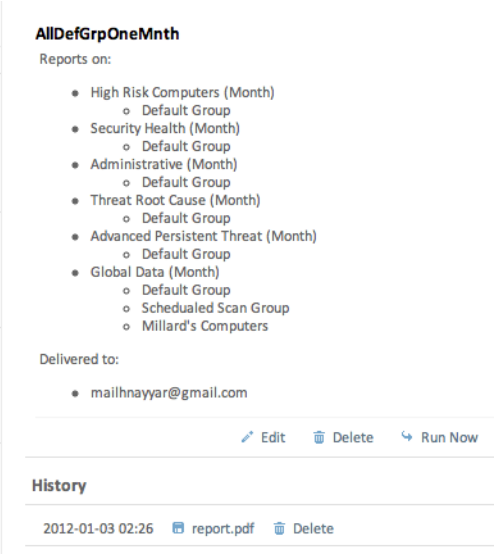
Saved Reports

After you have saved a report it will be available on the main Reports screen. You can see the name of the report, description, the date the report was created, the next date it will run, and the last date it was run. You can also edit the report settings, delete the report entirely, or run the report. Note that deleting a report will not delete previous instances of the report that were run from the report history.



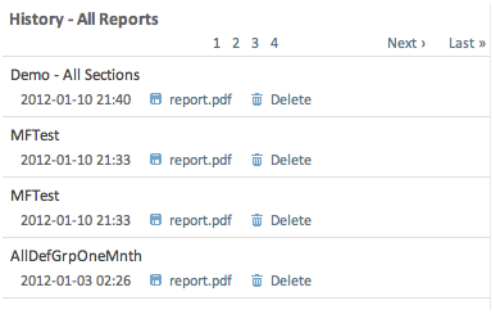
Clicking on the name of a report will provide a summary of the report along with information on who the report will be delivered to. A history of that particular

report is available that allows you to download previous instances of the report or delete them.



History - All Reports

All reports that have been previously generated can be accessed in this area of the Reports page. From here you can download previous reports or delete them.



CHAPTER 18
ACCOUNTS

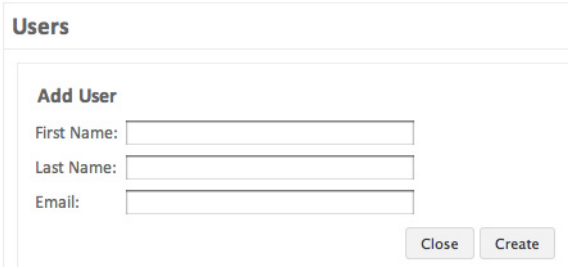
Items under the Accounts menu allow you to manage your FireAMP console. User management, defaults, and audit logs can all be accessed from this menu.

Users

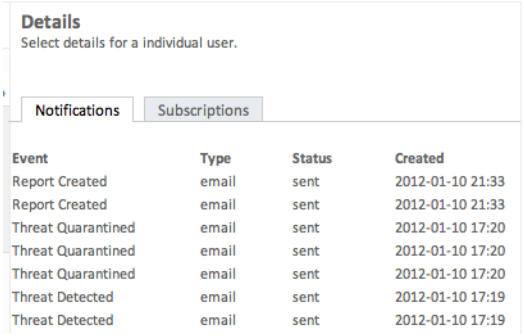
The Users screen allows you to manage accounts and view notifications and subscriptions for that account.

You can navigate through the user list using the links at the top of the list. When you select an account you can see different options for it including options to edit or delete the account. If you select your own account you also have the option to reset your password.

Click on Add User to create a new FireAMP console user account. A valid email address is required for them to receive an account activation email.



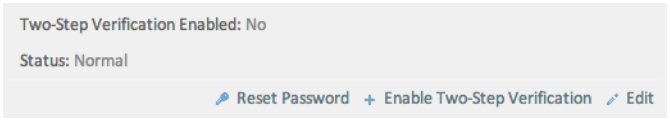
When you select a user account you can also view the Notifications and List View for that user. The Notifications list displays any events sent to the user such as forgotten password reset messages, subscription emails, and report creation messages.



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 Two-Step Verification** on your account in the Users page.

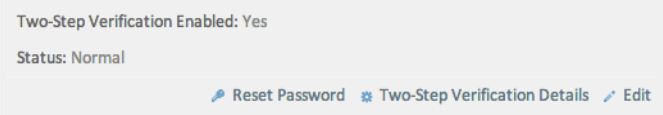


You will then be guided through the steps to enable two-step verification on your account, including backup codes. It is important to keep a copy of your backup

codes in a safe location in case you are unable to access the device with your authenticator app.

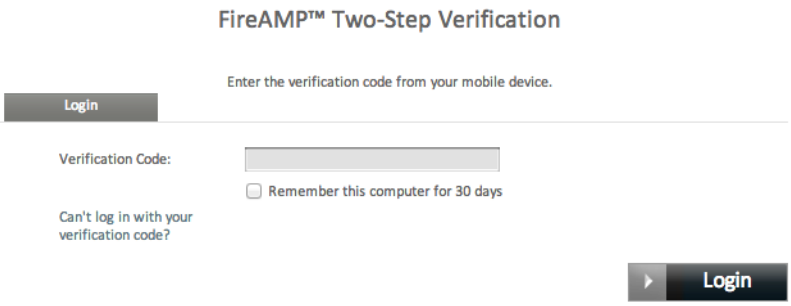
IMPORTANT! Each backup code can only be used one time. After you have used all your backup codes you should return to this page to generate new ones.

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.

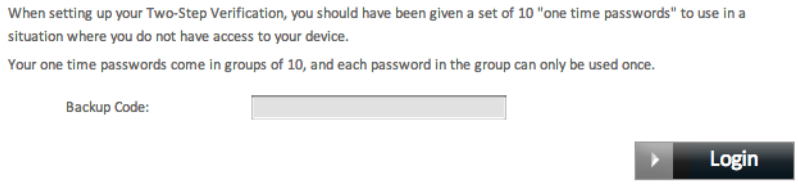
The next time you log in to the FireAMP console you will be prompted for your verification code after you enter your email address and password.



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.

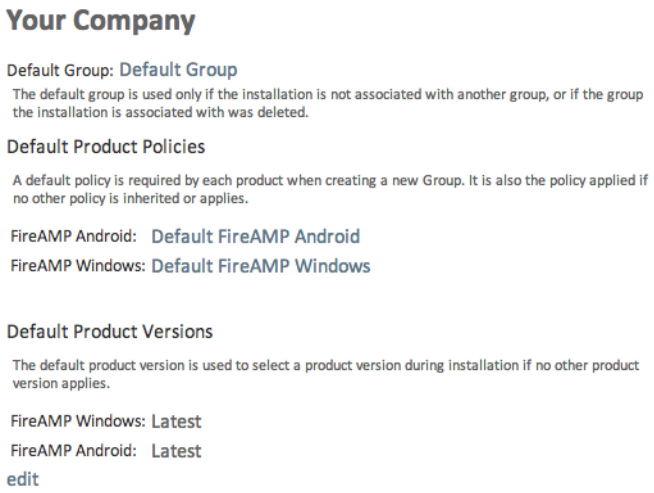


If you do not have access to your authenticator device or your backup codes you will need to contact Sourcefire Support.

Business

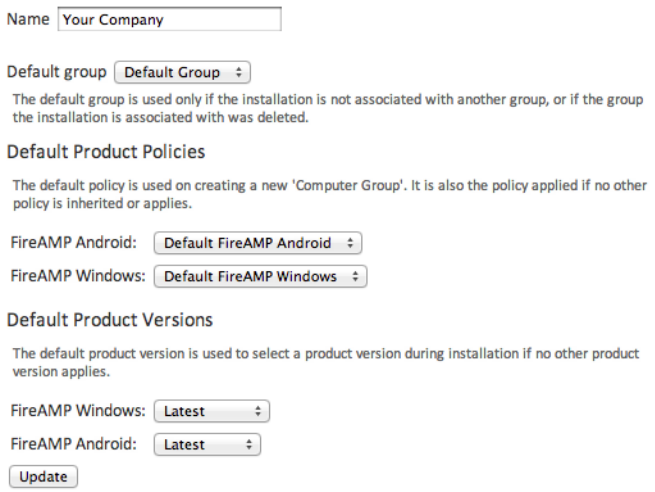
The Business screen allows you to specify global defaults for your FireAMP deployment and displays your current license status.

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. Clicking the edit link allows you to make changes.

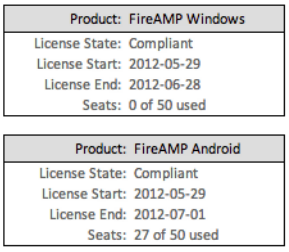


The Name entry appears on all reports that are generated from your FireAMP deployment. You can also change the Default Group that computers not assigned a group will be a part of. Similarly, the Default Policy defines the initial policy for any new groups that are created unless one is specified or they 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.



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.

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.

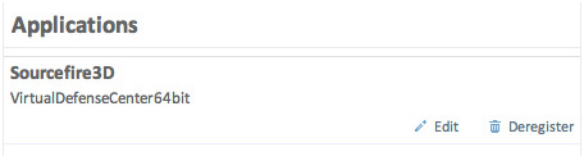
When the Demo Data has been enabled you can click **Disable Demo Data** to remove it again.

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

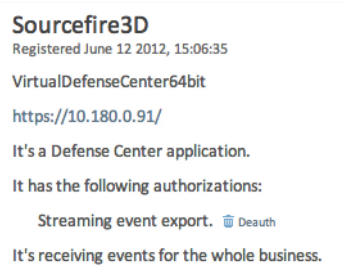
The Applications menu shows which applications external to FireAMP that you have authorized to access your organization's data. For example, you can display FireAMP data in your Sourcefire Defence Center dashboard. For more information on Defence Center integration with FireAMP see your Defence Center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

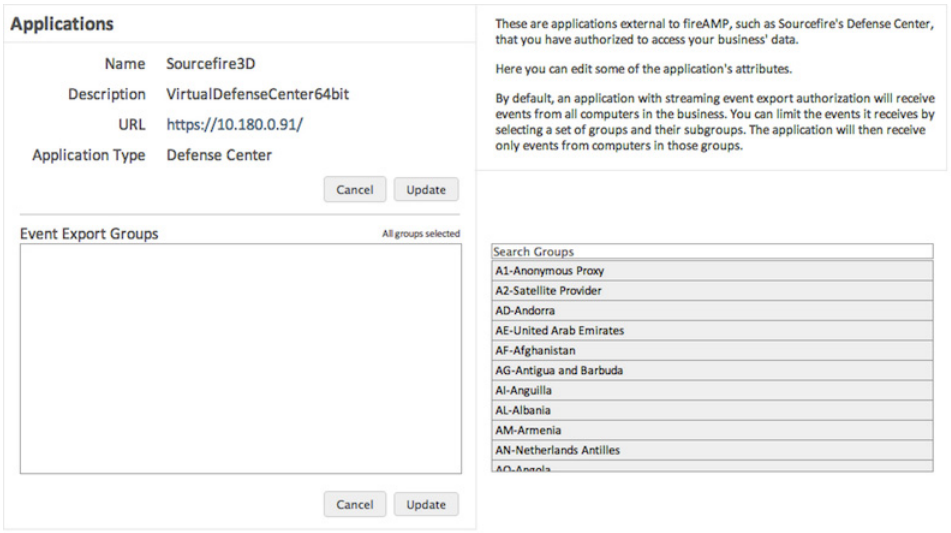
When you select the name of an application from your list you will see the current settings for that application.



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.

APPENDIX A
THREAT DESCRIPTIONS

FireAMP has unique network detection event types and Indications of Compromise. Descriptions of these detection types are found in this section.

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.

- [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.

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 Custom Whitelists.

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 Sourcefire Intelligence Feed, custom IP lists you create, or a combination of both. DFC detections include:

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

Appendix B
Supporting Documents

The following supporting documents are available for download.

Sourcefire FireAMP 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

Sourcefire FireAMP 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

Sourcefire FireAMP Release Notes

The Release Notes contain the FireAMP change log.

Download the Release Notes

Sourcefire 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 SF-EICAR document

Download the ZAccess document

Download the ZBot document

APPENDIX C
SUBSCRIPTION AGREEMENT

SUBSCRIPTION AGREEMENT

Sourcefire FireAMP Products

IMPORTANT: PLEASE READ THIS AGREEMENT CAREFULLY.

THIS SUBSCRIPTION AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU, THE END USER CUSTOMER ("YOU"), AND SOURCEFIRE, INC. OR ONE OF ITS DESIGNATED SUBSIDIARIES INSTEAD OF SOURCEFIRE, INC. (COLLECTIVELY, "SOURCEFIRE"), THAT IS ALLOWING YOU, ON A SUBSCRIPTION BASIS, TO ACCESS AND USE THE FIREAMP PRODUCTS.

IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. YOU AGREE THAT THIS AGREEMENT WITH SOURCEFIRE IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU.

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO ALLOW YOU TO USE THE FIREAMP PRODUCTS, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE FIREAMP PRODUCTS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF ANY OF THE FIREAMP PRODUCTS. BY CLICKING OR SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE FIREAMP PRODUCTS IN ANY WAY, OR BY EXECUTING AN ORDER THAT REFERENCES THIS AGREEMENT, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE

Appendix C

TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE FIREAMP PRODUCTS.

This Agreement governs Your access and use of the FireAMP Products unless there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the FireAMP Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separately signed written agreement, and (2) this Agreement.

1. DEFINITIONS

Unless otherwise defined herein, the capitalized terms used in this Agreement shall be defined in the context in which they are used. The following capitalized terms shall have the following meanings in this Agreement:

"Administrator" means the individual(s) permitted by You to access and use the Management Console.

"Agent Software" means the machine-readable software programs licensed by Sourcefire to You hereunder, including any pertinent Updates, which are installed on Your Endpoints.

"Documentation" means written information contained in user manuals and technical specifications pertaining specifically to the use of the FireAMP Products and made available by Sourcefire with the FireAMP Products in any manner (including on CD-ROM or on-line), including any pertinent Updates thereto.

"Endpoint" means any device capable of processing data including but limited to personal computers, mobile devices and networked computer workstations.

"FireAMP Products" means the Sourcefire proprietary advanced malware protection products consisting of the software hosted by Sourcefire and provided on a software as a service (SaaS) basis, the Licensed Materials and the Management Console.

"Laws" means, collectively, all international and national laws, treaties, statutes, ordinances, regulations and other types of government authority.

"Licensed Materials" means any Agent Software, Documentation, content and data made available to You by Sourcefire for Your use as part of the FireAMP Products.

"Management Console" means the user interface portion of the FireAMP Products accessible via a web browser which may be used by the Administrator to manage the use of the FireAMP Products.

"Party" or "Parties" means, individually each party hereto, and collectively all the parties to this Agreement.

"Reseller" means a reseller or distributor authorized by Sourcefire to sell and/or license Sourcefire products.

"Subscription" means Your right for a specified period of time that You will be permitted to access and use the FireAMP Products.

"Subscription Fee" means the fee required to be paid by You to use the FireAMP Products during the term of the Subscription. The Subscription Fee must be paid directly to Sourcefire or to a Reseller. The Subscription Fee will be as set forth in Your order to Sourcefire or Reseller, as applicable.

"Third Party Products" means any products or other materials made available to You for use with Sourcefire Products and which are not Sourcefire products.

"Updates" means with respect to Licensed Materials any Sourcefire-approved periodic patches, bug-fixes, work-arounds, error corrections, enhancements, software updates, Documentation revisions, and additions and other modifications thereto, or revised versions thereof, which are made available from time to time.

2. YOUR PAYMENT OBLIGATIONS

In consideration for Your right to use the FireAMP Products during the Subscription, You agree to pay the applicable Subscription Fees and all applicable taxes and any late payment fees.

3. LICENSE GRANT

Subject to the terms and conditions of this Agreement, Sourcefire grants to You a limited, non-exclusive and non-transferable right and license during the term of the Subscription to (i) download, install and use the Agent Software on the number of Endpoints for which You have paid the required Subscription Fee(s), (ii) use the Licensed Materials solely as part of Your use of the FireAMP Products and solely for internal security purposes, and (iii) access and use the Management Console solely as part of Your use of the FireAMP Products and solely for internal security purposes. You may not use the FireAMP Products in a manner that exceeds the permitted number of Endpoints, term of the Subscription, or other limitations associated with the applicable Subscription Fee(s) paid or payable by You. You may increase Your number of Endpoints by paying the applicable additional Subscription Fee(s). You may be required to input a registration number, product authorization key or otherwise register online at Sourcefire's designated website to obtain the necessary license key or license file to download and install the Licensed Materials. Sourcefire and Sourcefire's licensors, as applicable, retain all title, copyright and other intellectual proprietary rights in, and ownership of, the Licensed Materials. Sourcefire and its licensors expressly reserve any rights in Licensed Materials not granted herein.

4. USE OF MANAGEMENT CONSOLE

Your Administrator(s) may only access and use the Management Console to use the FireAMP Products and for no other purpose. You may create unique passwords and usernames to access the Management Console, in addition to allowing different users different levels of access to the Management Console. The Documentation shall set forth any browser-specific limitations for the Management Console.

5. LICENSE RESTRICTIONS

You agree not to directly or indirectly: (i) sell, lease, rent, distribute, sublicense or transfer the FireAMP Products or any portion thereof to a third party; (ii) allow any

third party to access or use the FireAMP Products other than Your employees or Your independent contractors that are providing services to You; (iii) reverse engineer, decompile, disassemble, decrypt or otherwise attempt to determine the source code of any of the Licensed Materials, or the Management Console, except to the limited extent permitted by Law; (iv) modify, make error corrections to or create derivative works based on the FireAMP Products; (v) use any portion of the FireAMP Products for the benefit of any third parties (e.g., in an ASP, SaaS, outsourcing or service bureau relationship) or in any way other than in its intended manner, except as otherwise permitted by Sourcefire; (vi) remove, alter or obscure any proprietary or copyright notice, labels, or marks on or within the FireAMP Products; (vii) copy, frame or mirror any part or content of the FireAMP Products; (viii) disable or circumvent any access control, license key or related security measure, process or procedure established with respect to the FireAMP Products; (ix) interfere with or disrupt the integrity or operation or use of any FireAMP Products by any other licensed user of the FireAMP Products or otherwise use any FireAMP Product to knowingly transmit malicious code to a third party with the intent to damage or otherwise harm such third party; or (x) access the FireAMP Products in order to build a competitive product. You may use the FireAMP Products to conduct internal performance and benchmark testing, the results of which only You may publish or publicly disseminate, provided that (a) Sourcefire has reviewed and approved the methodology, assumptions and parameters of Your testing, (b) You publish a full description of the test environment and methods, assumptions and parameters used in the testing, and (c) You do not publish false, deceptive or misleading statements relating to the test or FireAMP Products. Please contact a Sourcefire technical support representative regarding approved testing methodology, assumptions and parameters. You are responsible for all use of the FireAMP Products obtained by You and for compliance with this Agreement; any breach of this Agreement or Your Subscription by You or other user in connection with Your Subscription shall be deemed to have been made by You.

6. INTELLECTUAL PROPERTY

This Agreement does not transfer to You any title or any ownership right or interest in the FireAMP Products, or any portion thereof, or in any other intellectual property rights of Sourcefire or Sourcefire's licensors. You acknowledge that the FireAMP Products contain, embody and are based upon patented or patentable inventions, trade secrets, copyrights and other intellectual property rights owned by Sourcefire and its licensors. Licensed Materials are licensed to You pursuant to this Agreement and not sold to You.

7. TECHNICAL SUPPORT

You may obtain technical support for FireAMP Products by enrolling in Sourcefire's customer support plan (the "Support Plan") by paying the then-applicable customer support fee. A copy of the current Support Plan terms and conditions is available on Sourcefire's customer support portal, currently located http://www.sourcefire.com/customer-support. All Updates received by You pursuant to the Support Plan shall be governed by, and licensed to You under, this Agreement. Certain Subscriptions may include the support fee as part of the

Subscription Fee in which case You will be automatically enrolled in the Support Plan provided You pay the applicable Subscription Fee.

8. CONFIDENTIALITY

As used herein, "Confidential Information" means any non-public technical or business information of one Party (the "Disclosing Party") disclosed or made available to the other Party (the "Receiving Party"), including without limitation, Your data and any information relating to Sourcefire's techniques, algorithms, software, know-how, current and future products and services, research, engineering designs, financial information, procurement requirements, business forecasts, marketing plans and information, the terms and conditions of this Agreement, and any other information of Sourcefire (or its licensors) that is disclosed to You. Confidential Information shall not include any information that (i) is or becomes generally known to the public without breach of this section of the Agreement by the Receiving Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of this section of the Agreement, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party. The Receiving Party will employ all reasonable measures to maintain the confidentiality of the Disclosing Party's Confidential Information, but in no event shall such measures be less than the measures the Receiving Party employs to protect its own Confidential Information. The Receiving Party will limit the disclosure of Confidential Information to its employees and contractors with a bona fide need to access such Confidential Information in order to exercise its rights and discharge its obligations under this Agreement; provided that, all such employees and contractors are bound by a written non-disclosure agreement that contains restrictions at least as protective as those set forth herein. Each Party agrees that the Disclosing Party will suffer irreparable harm in the event that the Receiving Party breaches any obligation under this Section 8 and that monetary damages will be inadequate to compensate the Disclosing Party for such breach. In the event of a breach, or threatened breach, of any of the provisions of this Section 8, the Disclosing Party, in addition to and not in limitation of any other rights, remedies or damages available to it at law or in equity, shall be entitled to seek a temporary restraining order, preliminary injunction and/or permanent injunction in order to prevent or to restrain any such breach.

In the event that the Receiving Party is required by Law to disclose any of Disclosing Party's Confidential Information, then the Receiving Party shall promptly notify Disclosing Party prior to making any such disclosure and provide reasonable cooperation to Disclosing Party in seeking a protective order or other appropriate remedy from the proper authority. Receiving Party further agrees that if Disclosing Party is not successful in precluding the requesting legal body from requiring the disclosure of the Confidential Information, it will furnish only that portion of the Confidential Information that is legally required, will promptly provide Disclosing Party with a copy of the information so furnished, and will exercise all reasonable efforts to obtain reliable assurances that the recipient will accord it confidential treatment.

9. DATA COLLECTION

Sourcefire hereby informs You that FireAMP Products use data collection technology to collect and analyze certain information about Your network and Endpoints including, but not limited to, the IP addresses of Your Endpoints and the metadata of certain executable files in order to identify malware on Your Endpoints, to provide related services to You and to improve Sourcefire's products. You do have the ability to configure the FireAMP Products to limit some of the data that can be collected. You grant Sourcefire a perpetual right and license to use the information and data made available by You via the FireAMP Products in order to attempt to prevent malware from running on Your Endpoints, to conduct related analysis and for product improvement purposes. By accepting this Agreement, You (i) acknowledge and agree that the technology included in the FireAMP Products can collect traffic and data from Your network and Endpoints to detect malware and conduct related analysis, (ii) agree to upload from Your network and Endpoints certain metadata and other required information for the purpose of being scanned by the remote cloud-based servers operated by Sourcefire, and (iii) covenant that You have the right to provide Sourcefire all such information and data. You further acknowledge and agree that Sourcefire may provide Updates to the FireAMP Products which may automatically download to your Endpoints.

10. INSTALLATION

You represent, warrant and covenant that You are solely responsible for the proper installation, configuration and management of the hardware on which the Licensed Materials will be installed, as well as the installation of any separately provided Licensed Materials. You further understand and hereby acknowledge that the failure to properly configure and manage Your hardware and Endpoints, and the failure to properly install any separately provided Licensed Materials, may adversely affect the performance of the FireAMP Products. You represent, warrant and covenant that You will adhere to the recommended operating requirements specified in the Documentation. Sourcefire shall have no obligation under this Agreement to the extent the FireAMP Products fail to substantially perform the functions described in the Documentation, in whole or in part, because (i) You fail to adhere to the specified operating requirements, (ii) Your hardware or Endpoints fail to perform properly, (iii) You mis-configured any portion of the FireAMP Products, or (iv) the Licensed Materials had been improperly installed. You further agree to indemnify and hold harmless Sourcefire, its Resellers and their respective officers, directors, employees and agents against any claims, losses, damages, liabilities or expenses arising from the failure of the FireAMP Products to perform as warranted where such failure to perform is attributable, in whole or in part, to (i) Your failure to adhere to the specified operating requirements, (ii) the failure of Your hardware or Endpoints to perform properly, (iii) Your mis-configuration of the FireAMP Products, or (iv) the improper installation of the Licensed Materials, provided, however, the foregoing indemnification obligation shall not apply if You are the U.S. government.

11. WARRANTIES AND DISCLAIMER

Sourcefire warrants that for a period of ninety (90) days from the date the FireAMP Product is made available to You for use, the unmodified FireAMP

Product will, under normal use, substantially perform the functions described in its Documentation. The aforementioned warranty shall not apply if any portion of the FireAMP Product (i) has been altered in a manner not recommended by the Documentation, except when altered by Sourcefire or its authorized representative, (ii) has not been installed, operated, repaired or maintained in accordance with instructions supplied by Sourcefire, or (iii) is licensed for beta, evaluation, testing or demonstration purposes.

EXCEPT AS EXPRESSLY WARRANTED IN THIS SECTION 11, THE FIREAMP PRODUCTS (INCLUDING, ANY EVALUATION AND BETA PRODUCTS), AND ANY OTHER DOCUMENTATION, MATERIALS AND/OR DATA PROVIDED BY SOURCEFIRE ARE PROVIDED "AS IS" AND "WITH ALL FAULTS," AND SOURCEFIRE EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND OR NATURE, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF OPERABILITY, CONDITION, TITLE, NON-INFRINGEMENT, NON-INTERFERENCE, QUIET ENJOYMENT, VALUE, ACCURACY OF DATA, OR QUALITY, AS WELL AS ANY WARRANTIES OF MERCHANTABILITY, SYSTEM INTEGRATION, WORKMANSHIP, SUITABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THE ABSENCE OF ANY DEFECTS THEREIN, WHETHER LATENT OR PATENT.

THE FIREAMP PRODUCTS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. FIREAMP PRODUCTS ARE NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, POWER GENERATION, AIR TRAFFIC CONTROL SYSTEMS, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, PHYSICAL INJURY OR PROPERTY DAMAGE.

NO WARRANTY IS MADE BY SOURCEFIRE ON THE BASIS OF TRADE USAGE, COURSE OF DEALING OR COURSE OF TRADE. SOURCEFIRE DOES NOT WARRANT THAT THE FIREAMP PRODUCTS OR ANY OTHER INFORMATION, MATERIALS, DOCUMENTATION OR TECHNOLOGY PROVIDED UNDER THIS AGREEMENT WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION THEREOF WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE CORRECTED. YOU ACKNOWLEDGE THAT SOURCEFIRE'S OBLIGATIONS UNDER THIS AGREEMENT ARE FOR YOUR BENEFIT ONLY. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ANY THIRD PARTY PRODUCTS ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER.

Sourcefire's sole obligation and liability, and Your sole and exclusive remedy under the warranties set forth in Section 11 shall be for Sourcefire to use commercially reasonable efforts to fix or replace the defective FireAMP Product, if Sourcefire is notified in writing of all warranty problems during the applicable warranty period.

12. LIMITATION OF LIABILITY

IN NO EVENT WILL SOURCEFIRE'S OR ANY OF ITS SUBSIDIARIES' OR AFFILIATES' AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO,

LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS AGREEMENT, OR THE USE OF THE FIREAMP PRODUCTS, EXCEED THE AMOUNT OF THE SUBSCRIPTION FEES YOU PAID TO SOURCEFIRE OR ITS RESELLER, AS APPLICABLE, FOR THE FIREAMP PRODUCTS THAT GAVE RISE TO SUCH LIABILITY. UNDER NO CIRCUMSTANCES SHALL SOURCEFIRE OR ANY OF ITS SUBSIDIARIES, AFFILIATES, SUPPLIERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS, EXCEPT AS SET FORTH IN SECTION 14; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA; (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS); OR (IV) DAMAGES ARISING OUT OF ANY THIRD PARTY PRODUCTS, IN EACH CASE EVEN IF SOURCEFIRE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM ANY PRODUCTS, AND FOR ANY RELIANCE THEREON, AND WHETHER YOUR USE OF THE FIREAMP PRODUCTS COMPLIES WITH APPLICABLE DATA PRIVACY LAWS. THE LIMITATIONS OF LIABILITY IN THIS SECTION 12 ARE INTENDED TO APPLY WITHOUT REGARD TO WHETHER OTHER PROVISIONS OF THIS AGREEMENT HAVE BEEN BREACHED OR HAVE PROVEN INEFFECTIVE.

13. ESSENTIAL BASIS

The disclaimers, exclusions and limitations of liability set forth in this Agreement form an essential basis of the bargain between the Parties, and, absent any such disclaimers, exclusions or limitations of liability, the provisions of this Agreement, including, without limitation, the economic terms, would be substantially different.

14. INFRINGEMENT OBLIGATIONS

14.1. Sourcefire will defend You from any unaffiliated third party claim that Your use of the FireAMP Products as provided by Sourcefire to You under this Agreement, when used within the scope of this Agreement, infringes any unaffiliated third party's U.S. copyright ("Claim"). Sourcefire's obligations to You under this Section 14 are limited solely to paying (i) counsel hired by Sourcefire to defend the Claim, (ii) the reasonable and verifiable out-of-pocket costs incurred directly by You in connection with defending the Claim and/or assisting Sourcefire in the defense thereof, and (iii) subject to Section 12 herein, any direct damages finally awarded to such third party by a court of competent jurisdiction (after any appeals) or any settlement of the Claim to which Sourcefire consents in writing. Sourcefire's obligations under this Section 14 are expressly contingent upon: (x) You giving prompt written notice to Sourcefire of any such Claim, (y) You allowing Sourcefire exclusive control of the defense and any related settlement of any such Claim, and (z) You furnishing Sourcefire with reasonable assistance in connection with the Claim without prejudicing Sourcefire in any manner. Subject to the foregoing conditions, nothing in this Agreement shall prohibit You from hiring separate counsel, at Your own expense.

14.2. If Your use of the FireAMP Products hereunder is, or in Sourcefire's opinion is likely to be, enjoined due to the type of Claim specified in Section 14.1, then Sourcefire may, at its sole option and expense but without obligation to do so: (i) procure for You the right to continue to use the FireAMP Products under the terms of this Agreement; (ii) replace the FireAMP Products with a functional equivalent; (iii) modify the FireAMP Products so that they become non-infringing (including disabling the challenged functionality), provided the modified products remain substantially equivalent in function to the enjoined products; or (iv) terminate Your Subscription with respect to the FireAMP Products that are subject to the Claim by providing thirty (30) days written notice and refund to You any prepaid Subscription Fees covering the remainder of the Subscription after the effective date of such termination. Further, if as a result of a Claim, a court of competent jurisdiction issues a final injunction (which has not been appealed) against Your use of any part of the FireAMP Products, Sourcefire will, at its sole option, perform one of the remedy options listed in this Section 14.2. In either case, if Sourcefire selects option (ii), (iii) or (iv) listed in this Section 14.2, You shall immediately refrain from use of the allegedly infringing FireAMP Products.

14.3. Sourcefire shall have no obligation or liability for any Claim to the extent that it arises out of or relates to: (i) Your use of the FireAMP Products after Sourcefire notifies You to discontinue use due to a Claim; (ii) the combination of the FireAMP Products with a non-Sourcefire application, product, data or business process; (iii) damages attributable to a non-Sourcefire application, product, data or business process; (iv) modifications to any portion of the FireAMP Products made other than by Sourcefire; (v) Your continued use of the FireAMP Products for which Sourcefire has provided You with modifications or substitute products if use of such modifications or substitute products would have prevented the Claim; or (vi) use of the FireAMP Products in a manner prohibited under this Agreement.

14.4. THE PROVISIONS OF THIS SECTION 14 SET FORTH SOURCEFIRE'S SOLE AND EXCLUSIVE OBLIGATIONS, AND YOUR SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT, VIOLATION OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF ANY KIND. IN NO EVENT SHALL SOURCEFIRE'S LIABILITY TO YOU UNDER SECTION 14 EXCEED THE AMOUNT OF THE SUBSCRIPTION FEES PAID BY YOU FOR THE FIREAMP PRODUCT THAT IS THE SUBJECT OF SUCH CLAIM.

15. USE VERIFICATION

You agree that Sourcefire or its designee shall have the right to annually conduct an audit of Your use of the FireAMP Products for the purpose of verifying that You are in compliance with Your obligations under this Agreement and have paid all applicable Subscription Fees. These audits will be conducted during regular business hours, and Sourcefire will make reasonable efforts to minimize interference with Your regular business activities. Alternatively, Sourcefire may request that You complete a self-audit questionnaire in a form provided by Sourcefire. If an audit or such questionnaire reveals unlicensed use of the FireAMP Products, You agree to promptly pay all unpaid Subscription Fees to permit all usage disclosed.

16. EXPORT; RE-EXPORT

The FireAMP Products are subject to export controls under the Laws of the United States and other countries. You shall comply with all such Laws governing export, re-export, transfer and use of the FireAMP Products and will obtain all required U.S. and local authorizations, permits and licenses. Sourcefire assumes no responsibility or liability for Your failure to obtain such necessary authorizations, permits and licenses. Information regarding U.S. export laws can be found at www.bis.doc.gov. You agree not to use or transfer the FireAMP Products for any use relating to the operation of nuclear facilities, power generation, chemical or biological weapons, or missile technology, unless authorized by the U.S. Government by regulation or specific written license.

17. U.S. GOVERNMENT END USERS

The FireAMP Products, information and data provided under this Agreement are prepared entirely at private expense and are "Commercial Items" as that term is defined in 48 C.F.R. 2.101. If you are an agency, department, or other entity of the United States Government, or funded in whole or in part by the United States Government, then your use, duplication, reproduction, release, modification, disclosure or transfer of this commercial product and data, is restricted in accordance with 48 C.F.R. §12.211, 48 C.F.R. §12.212, 48 C.F.R. §227.7102-2, and 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.211, 48 C.F.R. §12.212, 48 C.F.R. §227.7102-1 through 48 C.F.R. §227.7102-3, and 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, this commercial product and data are licensed to U.S. Government end users (i) only as Commercial Items, and (ii) with only those rights as are granted to all other users pursuant to the standard user agreement for FireAMP Products. In case of conflict between any of the FAR and DFARS provisions listed herein and this Agreement, the construction that provides greater limitations on the U.S. Government's rights shall control. For purpose of any public disclosure provision under any federal, state or local law, it is agreed that this commercial product and data are a trade secret and proprietary commercial products and not subject to disclosure.

18. FREE SOFTWARE

You acknowledge and agree that while certain open source Third Party Products are made available to You hereunder for free for use in combination with the FireAMP Products, the terms and conditions under which such Third Party Products are being made available to You are as set forth in their respective third party agreements (the "Third Party Agreements"), and that this Agreement in no way supplements or detracts from any term or condition of such Third Party Agreements. Sourcefire is not giving any warranties for these Third Party Products and Your use of these Third Party Products will be subject solely to such Third Party Agreements. Sourcefire will pass any Third Party Product warranties through to You to the extent Sourcefire is authorized to do so under their respective Third Party Agreements. A listing of these Third Party Products, including the applicable Third Party Agreements and other applicable disclosures, is available in the Documentation. You may obtain the source code to such open source code software in accordance with the directions set forth in the Documentation.

19. EVALUATION PRODUCTS

If You have been provided FireAMP Products on an evaluation-only basis or beta-release basis (each, "Evaluation Products") to evaluate their suitability for use on a for-fee basis (as the case may be, for "Evaluation"), You acknowledge and agree that the evaluation license key(s) for these Evaluation Products may be set with a set expiration date (the "Expiration Date"), pursuant to which upon activation of the Evaluation Products, You may use the Evaluation Products through the Expiration Date (the "Evaluation Period") solely for their Evaluation. All Evaluation Products are provided to You "AS IS" without warranty or any kind, whether express, implied, statutory, or otherwise, and the limited warranties referenced in Section 11 and the indemnification obligations referenced in Section 14 above will not be applicable to Your use of the Evaluation Products. Sourcefire bears no liability for any damages resulting from use (or attempted use) of the Evaluation Products.

20. GOVERNING LAW

This Agreement shall be governed in all respects by the laws of the State of New York, USA, without regard to choice-of-law rules or principles. You expressly agree with Sourcefire that the U.N. Convention on Contracts for the International Sale of Goods shall not govern this Agreement. You represent that You understand, and You hereby agree to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable Laws. Except for instances where equitable relief is permitted under this Agreement, any and all claims, disputes, or controversies arising under, out of, or in connection with this Agreement or the breach thereof (each, a "Dispute") shall be submitted to the chief operating officer (or equivalent) of each Party (or their designee) for a good faith attempt to resolve the Dispute. The position of each Party shall be submitted, and the individuals promptly thereafter shall meet at a neutral site in an attempt to resolve such Dispute.

21. ASSIGNMENT

You may not assign or otherwise transfer this Agreement, or your Subscription, without Sourcefire's prior written consent. Notwithstanding the foregoing, You may assign this Agreement, and Your Subscription, if a majority of Your outstanding voting capital stock is sold to a third party, or if You sell all or substantially all of Your assets or if You otherwise undergo a change of control, provided, that, in such instance such assignment will not become effective until You provide Sourcefire written notice of such event. Sourcefire may assign or transfer this Agreement, in whole or in part, at any time in its sole discretion without Your consent. This Agreement shall be binding upon and inure to the benefit of the Parties' successors and permitted assigns.

22. CLAIMS AGAINST RESELLERS

This Agreement is for the benefit of Sourcefire and You, and is not intended to confer upon any other person or entity, including without limitation, any current or future Reseller, any rights or remedies hereunder. You agree that You shall not make any claim, demand, or take any action, or threaten to do the same, against any third party, including without limitation, any of Sourcefire's Resellers, for any actual or alleged breach of this Agreement, and You agree to defend, indemnify

and hold harmless Sourcefire, its Resellers and their respective officers, directors, employees, agents, resellers, distributors and subcontractors from any losses, damages, costs, liabilities or expenses attributable to Your breach of this Section 22, including reasonable attorneys fees and costs. The indemnification obligation in this Section 22 shall not apply to You if You are the U.S. Government.

23. TERM; TERMINATION

This Agreement will continue in effect during the term of Your Subscription and any renewal thereof, subject to the right of either Party to terminate as provided herein. Either Party may terminate this Agreement if the other does not comply with any of its terms, if the one who is not complying is given written notice and reasonable time to comply. Sourcefire may terminate Your Subscription and access to the FireAMP Products immediately if You breach any of the terms or conditions of Sections 2-5 of this Agreement. You agree that, upon such termination, You will cease using the Licensed Materials and either destroy or return all copies thereof.

24. GENERAL

This Agreement and the terms and conditions referenced herein are the Parties' complete agreement regarding its subject matter, superseding any prior oral or written communications. Under no circumstances will the terms of any purchase order issued by You control or otherwise negate the terms set forth in this Agreement. If any provision of this Agreement is held to be illegal or unenforceable for any reason, then such provision shall be deemed to be restated to be enforceable to the maximum extent permissible under Law, and the remainder of this Agreement shall remain in full force and effect. Neither Party shall be liable for any delay or failure due to a force majeure event and other causes beyond its reasonable control, provided, however, this provision shall not apply to Your payment obligations. Any notices under this Agreement to Sourcefire will be personally delivered or sent by certified or registered mail, return receipt requested, or by nationally recognized overnight express courier, to 9770 Patuxent Woods Drive, Columbia, Maryland U.S.A. 21046 or such other address as Sourcefire may specify in writing. Such notices will be effective upon receipt, which may be shown by confirmation of delivery. All notices to Sourcefire shall be sent to the attention of General Counsel (unless otherwise specified by Sourcefire). Amendments or changes to this Agreement must be in mutually executed writings to be effective. Sections 1-2, 5-6, 8, 11-13, 15, 20, 22 and 24, shall survive the termination or expiration of this Agreement. The Parties are independent contractors for all purposes under this Agreement.

--END OF AGREEMENT--

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

Z