Sourcefire FireAMP
Deployment Strategy

Version 4.5
Table of Contents

Chapter 1: Planning........................................................................................................... 3
  System requirements and supported operating systems........................................... 4
  Incompatible software and configurations............................................................ 5
  Gather information about endpoint security......................................................... 5
  Create exclusions for FireAMP in other security products .................................... 6
    Creating Exclusions in McAfee Products......................................................... 6
    Creating Exclusions in Symantec Products...................................................... 7
    Creating Exclusions in Microsoft Security Essentials.......................................... 7
  Gather information about custom apps ................................................................... 8
  Gather information about proxy servers ............................................................... 8
  Check firewall rules............................................................................................... 9
  Selecting computers for evaluation deployment .................................................. 9

Chapter 2: Portal Configuration ........................................................... 10
  Create exclusions ............................................................................................... 10
  Create outbreak control lists............................................................................... 12
  Create policies .................................................................................................... 13
  Create groups ..................................................................................................... 15
  Create whitelist from gold master....................................................................... 16
  Download installer .............................................................................................. 16

Chapter 3: Deploying the FireAMP Connector ................................... 18
  Command line switches ..................................................................................... 18
    Installer exit codes....................................................................................... 19
  Deployment ........................................................................................................ 20
    Microsoft System Center Configuration Manager ........................................... 20

Chapter 4: Troubleshooting................................................................. 27
  Initial Configuration Failure ................................................................................. 27
  Performance ........................................................................................................ 27
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook performance</td>
<td>28</td>
</tr>
<tr>
<td>Cannot connect to the cloud</td>
<td>28</td>
</tr>
<tr>
<td>Copy, move, or execute events not in Device Trajectory</td>
<td>29</td>
</tr>
<tr>
<td>Network events not in Device Trajectory</td>
<td>30</td>
</tr>
<tr>
<td>Policy not updating</td>
<td>30</td>
</tr>
<tr>
<td>Proxy</td>
<td>31</td>
</tr>
<tr>
<td>Simple Custom Detections</td>
<td>32</td>
</tr>
<tr>
<td>Custom Whitelists</td>
<td>32</td>
</tr>
<tr>
<td>Application Blocking</td>
<td>33</td>
</tr>
<tr>
<td>Contacting Sourcefire Support</td>
<td>33</td>
</tr>
</tbody>
</table>

Appendix A: Subscription Agreement ................................. 35
This document will guide you through best practices to deploy FireAMP for the first time. Following this strategy will increase your chances of a successful FireAMP deployment and evaluation.

Before deployment you should gather as much information as possible about the environment to reduce post-install troubleshooting. To have an effective roll out of the FireAMP Connector for Windows, you must first identify your environment. To do that you must answer the following questions:

- How many computers is the FireAMP Connector for Windows being installed on?
- Which operating systems are the computers running?
- What are the hardware specifications for the computers?
- Do the operating systems and specifications meet the minimum requirements for the FireAMP Connector for Windows?
- Which applications are installed on the computers?
- Which custom applications or not widely deployed applications are installed on the computers?
- Do the computers connect to the Internet through a proxy?
- Will the FireAMP Connector be deployed on any Windows servers?
- What tool is being used to push software out to the endpoints?
- What security products (AV, HIDS, etc.) are installed on the computers?
- Do you want your users to see the FireAMP Connector user interface, desktop icon, program group and/or right-click menu?
Once you identify the environment you’re working with then you can apply your first best practice of identifying candidates for an Alpha release. The best way to choose your candidates for Alpha is to choose a combination of three computers per operating system, three computers per custom application, three computers per proxy server, one computer per security product, and one computer per department. Your Alpha release should probably contain a cross-section of approximately 100 computers.

System requirements and supported operating systems

The following are the minimum system requirements for the FireAMP Connector based on the operating system. Operating systems not listed here are not currently supported. 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**
- 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 (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
Planning
Incompatible software and configurations

• 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.

**Gather information about endpoint security**

Conflicts can arise when multiple security applications are running on a single computer. To prevent conflicts between applications you will need to create exclusions for FireAMP in other security apps and exclude the security apps from FireAMP.

First, find out how many security applications are installed. Do different groups in the organization use different products? Find out the install, update, data, and quarantine path for each security product installed and make a note of it.

Next, decide on the install path for the FireAMP Connector. By default this is C:\Program Files\Sourcefire. You will need to exclude the FireAMP Connector directory from the other security applications, particularly antivirus products.
Create exclusions for FireAMP in other security products

Creating Exclusions in McAfee Products

**ePolicy Orchestrator 4.6**
1. Log in to ePolicy Orchestrator.
2. Select Policy > Policy Catalog from the Menu.
3. Select the appropriate version of VirusScan Enterprise from the Product pulldown.
5. Select the Exclusions tab click the Add button.
6. In the By Pattern field enter the path to your FireAMP Connector install (C:\Program Files\Sourcefire by default) and check the Also exclude subfolders box.
7. Click OK.
8. Click Save.
10. Repeat steps 5 through 8 for this policy.

**VirusScan Enterprise 8.8**
1. Open the VirusScan Console.
3. Select All Processes from the left pane.
4. Select the Exclusions tab.
5. Click the Exclusions button.
6. On the Set Exclusions dialog click the Add button.
7. Click the Browse button and select your FireAMP Connector install directory (C:\Program Files\Sourcefire by default) and check the Also exclude subfolders box.
8. Click OK.
9. Click OK on the Set Exclusions dialog.
Creating Exclusions in Symantec Products

Managed Symantec Enterprise Protection 12.1
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.

Unmanaged Symantec Enterprise Protection 12.1
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 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 or agent.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.

---

### Gather information about custom apps

Custom applications can present a problem for initial deployment. Most widely-used applications have already been marked as clean files in the FireAMP Cloud and tested with the FireAMP Connector. Custom applications are less likely to have this benefit, so extra precautions need to be taken with them. Find out if there are any custom or legacy applications running and the install path for each one and make a note of it. If only certain groups of users have the application installed, note which users they are. If the custom application has separate information stores, note the file path of those as well.

If possible, use a program like md5deep to calculate the SHA-256 value of the custom application’s executable files.

---

### Gather information about proxy servers

If the computers in the organization use a proxy server to connect to the Internet you will need to gather some information about it including:

- Proxy host name
- Proxy port
- Type of proxy
- User name and password for authentication (if required)
- PAC file URL if they are used
- Whether the proxy server is used for DNS resolution
- If the proxy server will allow communications via TCP port 32137
Check firewall rules

To allow the Connector to communicate with Sourcefire 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

Selecting computers for evaluation deployment

Instead of installing the FireAMP Connector on a single computer, select a representative cross section of different users. If different operating systems and application sets are in use, try to deploy on at least one of each image type.
Before deploying FireAMP Connectors there are tasks to complete in the FireAMP portal based on the information you gathered.

Create exclusions

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

The first step is to create an exclusion by navigating to Management > Exclusions in the FireAMP console.
Portal Configuration
Create exclusions

Click on **Create Exclusion Set** to create a new list of exclusions. Enter a name for the list - for example, Desktop Exclusions - and click **Create**.

Next click **Add Exclusion** to add an exclusion to your list.

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. More information about CSIDLs can be found [here](#). Common CSIDLs are:

**Symantec Endpoint Protection:**
- `CSIDL_COMMON_APPDATA\Symantec`
- `CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection`
- `CSIDL_PROGRAM_FILESx86\Symantec\Symantec Endpoint Protection`
- `CSIDL_COMMON_APPDATA\Symantec`

**McAfee VirusScan Enterprise:**
- `CSIDL_COMMON_APPDATA\VSE`
- `CSIDL_PROGRAM_FILES\VSE`
Portal Configuration
Create outbreak control lists

Trend Micro
- CSIDL_PROGRAM_FILES\Trend Micro
- CSIDL_PROGRAM_FILESX86\Trend Micro

Microsoft ForeFront
- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILESX86\Microsoft Forefront

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

Sophos
- CSIDL_PROGRAM_FILES\Sophos
- CSIDL_PROGRAM_FILESX86\Sophos

Splunk:
- CSIDL_PROGRAM_FILES\Splunk

**IMPORTANT!** CSIDLs are case sensitive.

Next create an exclusion set for your servers and another one for your Active Directory domain controllers. Make sure to exclude any security products as you did in your desktop exclusions above and also create exclusions based on your server roles (Active Directory, file server, DHCP, etc.) and installed software (Exchange, SQL, IIS, etc.). Microsoft has compiled a list of links to exclusions for their server products at [http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx](http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx).

Create outbreak control lists

During the early stages of deployment you may encounter previously unseen malware on computers as well as false-positive detection of custom applications. To make sure the FireAMP Connector deals with these properly, you will want to create a Simple Custom Detection list and a Custom Whitelist to associate with your policies.

To create a Simple Custom Detection list, go to Outbreak Control > Simple. Click Create to create a new Simple Custom Detection, name it Quick SCD (or a name that you prefer), and click on Save.

To create a Custom Whitelist, go to Outbreak Control > Whitelisting. Next click Create to create a new Custom Whitelist, name it Quick WL (or a name that you prefer), and click Save.
Create policies

For initial deployment we recommend you go to Management > Groups and create the following policies with specific configurations:

Audit Only
This policy puts the FireAMP Connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected but not blocked.
- This policy uses all the default policy settings but with the File > Modes > File Conviction Mode set to Audit.
- The proxy server information gathered previously should be entered under General > Proxy Settings.
- Associate the exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Protect
This is the standard policy for the FireAMP Connector that will quarantine malicious files and block malicious network connections. Once you have become familiar with the way the FireAMP Connector behaves you can tweak this policy to your own preferences.
- This policy uses all the default policy settings.
- The proxy server information gathered previously should be entered under General > Proxy Settings.
- Associate the exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Triage
This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected with malware.
- This policy uses all the default policy settings but with the File > Engines > Offline Engine set to TETRA and with Network > Device Flow Correlation (DFC) > Detection Action set to Block.
- The proxy server information gathered previously should be entered under General > Proxy Settings.
- Associate the exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.
Server

This is a lightweight policy for high availability computers and servers that require maximum performance and uptime.

- This policy uses all the default policy settings but with the File > Modes > File Conviction Mode set to Audit.
- If your servers are running Windows 2008 you must make sure that File > Engines > Offline Engine is set to Disabled.

**WARNING!** When installing the FireAMP Connector on a server you must also use the /skiptetra command line switch along with this policy setting.

- If your servers host services or applications that require a large number of network connections (SMB, SQL, Exchange, etc.) it is recommended that Network > Device Flow Correlation (DFC) > Enable DFC be unchecked.

**WARNING!** When installing the FireAMP Connector on a server you must also use the /skipdfc command line switch along with this policy setting.

- The proxy server information gathered previously should be entered under General > Proxy Settings.
- Associate the server exclusion set you previously created with this policy.
- Associate the Quick SCD list you created with this policy.
- Associate the Quick WL list you created with this policy.

Domain Controller

This is a lightweight policy for use on Active Directory Domain Controllers.

- This policy uses all the default policy settings but with the File > Modes > File Conviction Mode set to Audit.
- Because of authentication traffic from your network it is recommended that Network > Device Flow Correlation (DFC) > Enable DFC be unchecked.

**WARNING!** When installing the FireAMP Connector on a domain controller you must also use the /skipdfc command line switch along with this policy setting.
Portal Configuration
Create groups

• If your servers are running Windows 2008 you must make sure that File > Engines > Offline Engine is set to Disabled.

**WARNING!** When installing the FireAMP Connector on a domain controller you must also use the /skiptetra command line switch along with this policy setting.

• The proxy server information gathered previously should be entered under General > Proxy Settings.
• Associate the domain controller exclusion set you previously created with this policy.
• Associate the Quick SCD list you created with this policy.
• Associate the Quick WL list you created with this policy.

**IMPORTANT!** If you have computers in multiple geographic locations using different proxy servers you will need to create the above policies for each location ie. Audit Only NYC and Audit Only London.

Create groups

Now that you have created the initial policies for your deployment you need to create groups to associate the policies with. Go to Management -> Groups and create the following groups:

**Audit Only**
• Associate this group with the Audit Only policy.
• This should be the first group that the workstations in your deployment belong to so that you can root out any false positive detections without the files being quarantined.
• You can also use the Audit Only group as a performance group for computers that require higher availability or perform intensive tasks like rendering graphics.

**Protect**
• Associate this group with the Protect policy.
• Once you are satisfied with the performance of the computers in your Audit Only group, you can move them to the Protect group for normal operation of the FireAMP Connector so that malicious files are quarantined and network threats are blocked.
Triage
- Associate this group with the Triage policy.
- Any computers with existing infections or computers you suspect of being heavily infected should be moved to the Triage group since this group has more aggressive malware scanning enabled.

Server
- Associate this group with the Server policy.
- All of your servers other than Active Directory domain controllers should be in this group.

Domain Controller
- Associate this group with the Domain Controller policy.
- All of your Active Directory domain controllers should be in this group.

**IMPORTANT!** If you created multiple policies for different geographic locations in the previous section, you will need to create multiple groups for each location as well ie. Protect NYC and Protect London.

Create whitelist from gold master

If you have a gold master image available it is advisable to use it to whitelist applications. You can use a tool like `md5deep` to generate SHA-256 values for all the applications and add them to your Quick WL whitelist.

Download installer

Now that you have created your policies and associated them with groups you can begin deploying the FireAMP Connector to the computers you identified in the information gathering stage. Go to `Management > Deployment > Download` and download a redistributable installer for the Audit Only, Triage, Servers, and Domain Controllers groups.

All of your average user computers should initially use the Audit Only installer. This will allow you to make sure that all of the necessary applications have been whitelisted and proper exclusions were created. Any detections will still trigger alerts in the FireAMP console but nothing will be quarantined or blocked. This ensures that in the case of a false positive detection that there are no disruptions in regular operations. If you see a false positive detection, add the application in question to your whitelist. Once you are satisfied with the performance of the FireAMP Connector you can move computers from the Audit Only group into the Protect group. The Protect group has the same policy settings as the Audit Only group.
group, except that malicious files will be quarantined and connections to malicious websites will be blocked.

Only use the Domain Controllers installer on your Active Directory domain controller servers. The policy for this group includes exclusions that are specific to servers that run directory services for your tree.

Use the Servers installer on all your other servers, such as file, SQL, and Exchange servers.
CHAPTER 3
DEPLOYING THE FIREAMP CONNECTOR

Now you are ready to begin deploying the FireAMP Connector to your evaluation computers.

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.
Deploying the FireAMP Connector
Command line switches

- /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 user’s computer that must be completed before installing.
- 16003 – Unsupported operating system (i.e. XP SP2, Win2000).
- 16004 – invalid user permissions (not running as admin).
Deployment

The FireAMP Connector can be deployed through email using the email deployment option under Management > Email in the FireAMP Console. You can also download the installer from Management > Download and make the file available on a file share, use login scripts to install it, or distribute it using enterprise software deployment tools.

Microsoft System Center Configuration Manager

To install the FireAMP Connector using Microsoft System Center Configuration Manager (SCCM) you will first need to download the redistributable installer for each of your groups.

1. Go to Management > Download and select one of your groups, make sure to check the Create Redistributable Installer box, then click Download. The downloaded file will include the name of the group to make it easily identifiable, for example Protect-FireAMPSetup.exe.

2. Create a FireAMP folder in the shared source file directory on your SCCM server and copy the installer files to that folder.

3. Next, open your Configuration Manager Console and navigate to Software Library > Overview > Application Management > Applications and create Application.

4. On the first screen of the Create Application Wizard, select “Manually specify the application information” and click Next.
5. Enter identifying information for your application package. If you plan to deploy multiple group versions of the FireAMP Connector it is a good idea to use the group name to easily differentiate them in your software library. When you have entered the necessary information, click Next.
6. Enter the information available to your users in the Application Catalog. When you have entered the necessary information, click Next.

7. On the Deployment Types screen click the Add button to launch the Create Deployment Type wizard.

8. Select “Manually specify the deployment type information” and click Next.
9. Enter the application name and select languages then click Next.
10. Enter the path to the installer files you downloaded for each of your groups in the Content location field. Enter the name of your executable installer file along with any command line switches you want to use in the Installation program field. You can also specify the Uninstall program and path (C:\Program Files\Sourcefire\FireAMP\3.1.4\uninstall.exe by default). Click Next to continue.

12. Select File System as the Setting Type, then File as the Type. Enter the path to where you plan on installing the FireAMP Connector on your endpoints (C:\Program Files\Sourcefire\FireAMP\3.1.4 by default), then enter sfc.exe in the File or folder name field. Click OK, then click Next on the Detection Method page.
13. Select Install for system as the Installation behavior and Only when a user is logged on for the Logon requirement. Select the Installation program visibility setting you want, then check Allow users to view and interact with the program installation. Click Next.

14. You can choose to specify any installation requirements or simply click Next on the Requirements screen.

15. Click Next on the Dependencies screen.

16. Review your settings on the Summary screen and if you are satisfied click Next.

17. Once the wizard has completed successfully click Close to return to the Create Application Wizard. Click Next.

18. Review your settings on the Summary screen and if you are satisfied click Next.

19. Once the wizard has completed successfully click Close.

Your application will now be listed in the Software Library. Deploy the content to your Deployment Point and select whether to deploy it to Users and Groups or Devices.
This section describes some issues that may arise after the FireAMP Connector is installed and remediation steps.

**Initial Configuration Failure**

**Performance**

FireAMP uses a filter driver to identify file copies, moves, and executes. This may cause additional file latency in some applications that have high I/O such as databases. To reduce latency you may need to determine what should be excluded from FireAMP:

1. Identify where the application files exist.
2. Determine where the data files are being used.
3. Exclude both of those locations.
4. If there are still issues with the given application, turn on debug logging in the policy for the FireAMP Connector.
5. Use the logs to determine any temporary files being used.
Another helpful tip is that if you download the latest version of sqlite3 (http://www.sqlite.org/download.html), you can use that to query the history and see files that are continuously being written to, for example:

```
sqlite3.exe "C:\Program Files\Sourcefire\fireAMP\history.db"
SQLite version 3.7.16.2 2013-04-12 11:52:43
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .headers on
sqlite> select filename, count(filename) from history group by filename order by count(filename) desc limit 10;
```

```
filename|count(filename)
\?\C:\WINDOWS\Tasks\User_Feed_Synchronization-{A1489466-0BD4-42D2-A8B6-864FEA527577}.job|1706
\?\C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-ms|341
\?\C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-839522115-1229272821-725345543-500UA.job|222
...```

The above data identifies some exclusions that may be worth implementing:

- **FilePath**: CSI DL WINDOWS\Tasks
- **FileExtension**: *.feed-ms

### Outlook performance

If you notice slow performance in Outlook with the FireAMP Connector installed, this may be from the high I/O on the .pst or .ost file. In this case, it is best to create an exclusion for all .pst and .ost files in the FireAMP Console. Go to Management > Exclusions and click Edit for the exclusion set you want. Click Add Exclusion and select File Extension from the Exclusion type drop down menu. Enter .pst in the field and click Create. Repeat this for the .ost file extension if you use Outlook with an Exchange server.

### Cannot connect to the cloud

There can be any number of reasons why the FireAMP Connector cannot connect to the cloud. The most common two are that there is a firewall preventing the
Troubleshooting
Copy, move, or execute events not in Device Trajectory

outbound connection or that the proxy server is not cooperating with the connection. In both cases, you want to start troubleshooting with these steps:

1. Make sure the sfc.exe process (or agent.exe for versions prior to 3.1.4) is running. Open the Task Manager, select Show processes from all users, and make sure there is an sfc.exe process (agent.exe for versions prior to 3.1.4) listed. If it is not, open the command prompt as an administrator and run `net start immunetprotect`.

2. Make sure that there is only one iptray.exe process listed in the Task Manager. If there is more than one iptray.exe process you will need to end both iptray.exe processes and restart the Connector user interface.

3. Make sure you can connect to cloud-ec.amp.sourcefire.com over the correct port. TCP port 443 or 32137 is defined in the policy under General > Proxy Settings > Cloud Communication Port. A simple telnet test should suffice if there is no proxy configured. If there is a proxy, see the Proxy section below.

4. If you’re still unable to connect, then uninstall the FireAMP Connector and reboot the computer. Afterwards go to the policy that you’re using and set General > Administrative Features > Connector Log Level to Debug. Then download the FireAMP Connector installer and re-install it. This will give additional information to send to diagnose the issue.

Copy, move, or execute events not in Device Trajectory

The copy, move, and execute events come up to the Connector through the Immunet Protect driver. Then the Connector passes this information off to the cloud servers to decide whether a file is malicious. Then the cloud server will load it into a database that Device Trajectory reads from. Therefore to troubleshoot what is going on:

1. Check if the driver is installed properly. If you run `fltmc instances` from the command line as an administrator, it will list the drivers installed and which drives it’s bound with. What you want to see is the ImmunetProtectDriver bound to all of the local hard drives (i.e. C:\, E:\, etc.).

2. Check to see if the policy has Monitor File Copies and Moves and Monitor Process Execution enabled under File > Modes. Without these enabled, we will not monitor these file operations.

3. Check to see if you can connect to the cloud.

4. In your policy, set General > Administrative Features > Connector Log Level to Debug to make sure that you are getting disp=1 or disp=3 in your logs. A disp=4 means it failed to look up the file to the cloud. That could be an unsupported file type or other reason.
5. If you’re connected to the cloud and seeing the dispositions of 1 or 3 coming back from the cloud, then take a support diagnostics and send it to support@sourcefire.com along with your external IP address and we can take a look from the backend.

**Network events not in Device Trajectory**

The network information is picked up by the DFC driver and sent to the FireAMP Connector. The Connector passes this information off to the cloud server to see whether or not that connection is malicious. In order to troubleshoot what is going on:

1. Check to see if the policy has “Enable DFC” on
2. Enable the “Connector Log Level” of Debug if you can see events that list the IP and port information.

**IMPORTANT!** FireAMP only monitors the first 100 connections after process execution. Therefore you need to make sure that you execute a new process after you start the FireAMP Connector. Internet Explorer will re-use processes for each new tab whereas Chrome will start a new process upon tab creation.

**Policy not updating**

When a Connector fails to receive policy updates the most common causes are network connectivity or proxy configuration. For network connectivity issues, see Proxy and Cannot connect to the cloud. If the proxy settings in the policy were mis-configured then most often you will have to uninstall the FireAMP Connector, reboot the computer, fix the proxy settings in the policy, download the FireAMP Connector installer again, then reinstall it. However, if you already have one computer installed in a group (you can move a computer into that group just for this purpose), then you can:

2. Find the policy you’re looking for and click on it (DO NOT click Edit) so that you see the preview on the right hand side and click the Download Policy XML File button. Once the XML file has been downloaded:
   - Stop the FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
   - In the install folder (C:\Program Files\Sourcefire\FireAMP\“), rename the existing policy.xml to policy.xml.bak
   - Copy the policy.xml that you downloaded to that folder and rename it policy.xml
• Start the FireAMP Connector by running `net start immunetprotect` from a command prompt as an administrator.

• Open the policy.xml in the file you downloaded and note the serial number.

• Change something on the policy in the portal then click Sync Policy in the FireAMP Connector Settings screen. Wait approximately 2 minutes then check to see if the serial number has changed.

Proxy

Not every organization allows direct outbound connections to the Internet but instead routes connections through a proxy so that they can filter and scan traffic. FireAMP supports proxies, but it is important to make sure the policies are configured correctly. In this case, it’s probably best to start the FireAMP Connector with General > Administrative Features > Connector Log Level set to debug in the policy. If there aren’t any obvious errors in the logs:

• Stop the FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.

• Close any unnecessary applications then install and run Wireshark on the computer you’re troubleshooting.

• Try to get a packet capture started between the proxy server and the outbound Internet connection using Wireshark.

• Make sure that the browser on your computer is configured with the same proxy configuration as the browser on the computer you’re troubleshooting. Test to make sure you can get to https://console.amp.sourcefire.com.


  • `CURL_APP = "curlpath\curl.exe"`
    Where curlpath is the path to your curl install directory.

  • `PROXY_SERVER = "http://x.x.x.x:yyyy"`
    Where x.x.x.x is the IP address of your proxy server and yyyy is the port used (normally 8080).

  • `PROXY_USER_PASS = "Domain\username:password"`
    Where Domain\username and password are the username and password you use to authenticate to the proxy server. If your proxy doesn’t require authentication you can leave this field empty.

Then you can run:

cscript FireAMP_Helper.vbs testproxy
Troubleshooting
Simple Custom Detections

- Start the FireAMP Connector by running `net start immunetprotect` from a command prompt as an administrator.
- Let the Connector run for approximately 5 minutes to generate traffic.
- Get a FireAMP diagnostics, the PCAP from the FireAMP Connector to the proxy, and the PCAP from the proxy to the Internet and send them all to support@sourcefire.com.

Simple Custom Detections

Simple Custom Detections allow you to manually blacklist files for detection. If File > Modes > File Conviction Mode is set to Audit, you’ll just be notified of the detection but if it’s set to Quarantine, the file will be quarantined. The most common issue is that you found a file, you copied it on your machine, you add it to a Simple Custom Detection, and then you can’t understand why it’s not being detected. There could be a few reasons:

1. The file is being excluded. Compare the path you’re running from with the path in your exclusions listed in the policy.xml. Don’t forget to look at file extension exclusions as well.

2. The file is in a signed Microsoft or Verisign Class 3 certificate. Right-click on the file and look at the properties. Check to see if there is a Digital Signature associated with it and who the issuer is. If it is Verisign and you’re sure it’s malware, upload it to Virus Total and then contact support@sourcefire.com.

3. The file is not associated with the correct policy. Make sure the SHA-256 for the file is in the correct Simple Custom Detection list. Make sure that Simple Custom Detection list is associated with the policy that the Connector is using.

4. The file has been cached. This is by far the most common issue. When you copied it onto your computer, you created a record for it in your cache.db. To remove this:
   - Stop the FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
   - Go to the install directory (C:\Program Files\Sourcefire\FireAMP) and remove the cache.* files.
   - Start the FireAMP Connector by running `net start immunetprotect` from a command prompt as an administrator.
   - Now re-copy the file in question and make sure it is detected.

Custom Whitelists

The Custom Whitelist allows you to whitelist a file to avoid detection. This can be done as part of collecting all files from a “Golden Image” or in the case of a false
positive. The most common issue here is caching because you had it previously on your computer and need to clear your cache.db:

1. Stop the FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
2. Go to the install directory (C:\Program Files\Sourcefire\FireAMP) and remove the cache.* files.
3. Start the FireAMP Connector by running `net start immunetprotect` from a command prompt as an administrator.
4. Now re-copy the file you created and make sure it’s not detected.

Another possible issue is that the Custom Whitelist is not associated with the correct policy or that the file SHA-256 is not on that list.

Application Blocking

Application Blocking allows you stop a file from executing without quarantining the file. If you add a SHA-256 to an Application Blocking list and it still executes, there could be a few reasons why this may occur:

1. The file is being excluded. Compare the path you’re running from with the path in your exclusions listed in the policy.xml. Don’t forget to look at file extension exclusions as well.
2. The file is not associated with the correct policy. Make sure the SHA-256 for the file is in the correct Simple Custom Detection list. Make sure that Simple Custom Detection list is associated with the policy that the Connector is using.
3. The file has been cached. This is by far the most common issue. When you copied it onto your computer, you created a record for it in your cache.db. To remove this:
   - Stop the FireAMP Connector by running `net stop immunetprotect` from a command prompt as an administrator.
   - Go to the install directory (C:\Program Files\Sourcefire\FireAMP) and remove the cache.* files.
   - Start the FireAMP Connector by running `net start immunetprotect` from a command prompt as an administrator.
   - Now re-copy the file in question and make sure it does not execute.

Contacting Sourcefire Support

If you have not had success with other troubleshooting measures, you may need to contact Sourcefire Support to resolve your issue. In order to speed up
turnaround time for your support case it is helpful to provide some information when opening the case.

1. Go to Management > Policies and edit the policy the FireAMP Connector you’re troubleshooting is in.

2. Under General > Administrative Features set Connector Log Level to Debug.

3. On the FireAMP Connector go to Settings and click Sync Policy.
   If you installed the Connector using the command line switch to disable the Start Menu items you can force a policy sync by opening a command prompt and entering:
   ```
   %PROGRAMFILES%\Sourcefire\FireAMP\x.x.x\iptray.exe -f
   ```
   Where x.x.x is the FireAMP Connector version number.

4. After the policy has synced allow the Connector to run for 5-10 minutes or perform the specific actions that are causing errors.

5. Open the Windows Start Menu and go to FireAMP Connector and click Support Diagnostic Tool. This will create a file on your desktop named Sourcefire_Support_Tool_2013_XX_XX_XX_XX_XX.7z where XX will represent the month, day, and time you ran the tool.
   If you installed the Connector using the command line switch to disable the Start Menu items you can run the Support Diagnostic tool by opening a command prompt and entering:
   ```
   %PROGRAMFILES%\Sourcefire\FireAMP\x.x.x\ipsupporttool.exe
   ```
   Where x.x.x is the FireAMP Connector version number.

6. If you are having connectivity issues with the FireAMP Connector, take a PCAP of any network activity.

7. Upload the diagnostic file and PCAP to the Sourcefire SSL server at https://uploads.sourcefire.com/uploads/ed14f406d34f0fbd7c1af84fe024bd1d and make sure to note the filenames when contacting support.

8. If the issue is a user interface bug or a problem with the FireAMP Console, take a screenshot of the problem and attach it to the email you send.

9. Email support@sourcefire.com with all relevant information to the issue, the filenames of any files you uploaded, and attach your screenshots if required. Also make sure to include information on the type of proxy and firewall you are using in the case of connectivity issues.
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 YOU 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
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--