Product Guide

McAfee® Plugins for Microsoft ISA Server 1.4.0 Software

Contents

Contents

Preface

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input` or `Path`	Commands and other text that the user types; the path of a folder or program.
`Code`	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
	**Note**: Additional information, like an alternate method of accessing an option.
	**Tip**: Suggestions and recommendations.
	**Important/Caution**: Valuable advice to protect your computer system, software installation, network, business, or data.
	**Warning**: Critical advice to prevent bodily harm when using a hardware product.

What's in this guide

This guide is organized to help you find the information you need.

This guide is intended for administrators and assumes you have a working knowledge of:

- McAfee® Web Gateway
- McAfee® Data Loss Prevention
- McAfee® SaaS Web Protection
- Microsoft ISA Server
- Microsoft Windows operating systems on which the plugins are installed
- ICAP
- Proxy chaining

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introducing McAfee Plugins for Microsoft ISA Server

The McAfee® plugins for Microsoft ISA Server contains two plugins that integrate McAfee® Web Gateway, McAfee® Data Loss Prevention, or McAfee® SaaS Web Protection with Microsoft ISA Server.

McAfee Web Gateway

You can use either the ICAP plugin or the proxy chaining plugin to filter web traffic from the Microsoft ISA Server through the McAfee Web Gateway appliance. For more information about McAfee Web Gateway, see the McAfee Web Gateway product documentation.

- **ICAP plugin** — Configure the ICAP plugin when you want to use the McAfee Web Gateway appliance to filter inbound and outbound web traffic. In this scenario, the ICAP plugin redirects web traffic from the Microsoft ISA Server to the McAfee Web Gateway appliance where the web traffic is filtered according to policies and rules set up on the appliance. The traffic is then sent back to the Microsoft ISA Server for final routing through the network.
- **Proxy chaining plugin** — Configure the proxy chaining plugin when you want to use the McAfee Web Gateway appliance as an upstream proxy server in your proxy chain environment. In this scenario, the plugin forwards the web traffic to the McAfee Web Gateway appliance where the traffic is filtered according to policies and rules set up on the appliance. The McAfee Web Gateway appliance then sends a response back to the Microsoft ISA Server indicating the action to take on the request.

McAfee Data Loss Prevention

You can use the ICAP plugin to redirect web traffic from the Microsoft ISA Server to the McAfee DLP appliance for web traffic content filtering.

ICAP plugin — Configure the ICAP plugin when you want to use the McAfee DLP appliance to filter outbound web traffic. In this scenario, the ICAP plugin redirects outbound web traffic from the Microsoft ISA Server to the McAfee DLP appliance where the web traffic is filtered according to policies and rules you have set up. The response from filtering is then sent back to the Microsoft ISA Server, which delivers it to the user. For more information about McAfee DLP, see the McAfee DLP product documentation.

McAfee SaaS Web Protection

Use the proxy chaining plugin to forward traffic from the Microsoft ISA Server to the McAfee SaaS Web Protection service for URL filtering on web traffic requests.

Proxy chaining plugin — Configure the proxy chaining plugin when you want to use the McAfee SaaS Web Protection service to filter outbound web traffic requests. In this scenario, the plugin adds McAfee SaaS Web Protection authorization to web traffic requests and forwards the requests upstream to the McAfee SaaS Web Protection service where URL filtering takes place. The McAfee SaaS Web

Protection service then sends a response back to the Microsoft ISA Server, which delivers it to the user. For more information about McAfee SaaS Web Protection, see the McAfee SaaS Web Protection product documentation.

See also

About the ICAP plugin on page 11
About the proxy chaining plugin on page 23

2 Installation

Use the information and tasks in this section to plan for installation, download the installation file, and install the plugins.

Contents

System requirements

Follow the guidelines in this section to ensure you have the necessary system setup.

To install and operate the plugin for Microsoft ISA Server, you must have the following:

- Microsoft ISA Server 2004 for Microsoft Windows Server 2003 SP2 (32-bit)
- Microsoft ISA Server 2006 for Microsoft Windows Server 2003 SP2 (32-bit)

You must have one of the following:

- A currently supported version of McAfee Web Gateway
- A currently supported version of McAfee Data Loss Prevention
- A valid McAfee SaaS Web Protection account

For more information about any of the other McAfee products listed, see their product documentation.

Download the installation file

Download the installation file for the plugins.

Before you begin

Verify your system meets the system requirements.

Task

1. Log on to the operating system as an administrator.
2. Go to http://www.mcafee.com/us/downloads and enter your grant number to access your product downloads.
3. Go to **McAfee Plugins for Microsoft ISA Server** and download the installation file.

You can now install the plugins.

Install the plugins

Install the plugins on the server.

Before you begin

You must uninstall any previous versions of the Webwasher ISA ICAP plugins before installing the McAfee Plugins for Microsoft ISA Server.

The installer automatically installs both the ICAP plugin and the proxy chaining plugin.

If you have an array environment, install the plugins on each member of the array.

Task

1. Log on to the operating system as an administrator.
2. Close any open Microsoft ISA Server management consoles.
3. Locate and run the installation file.
4. Follow the prompts to install the plugin software.

The plugins are installed. By default, both plugins are enabled, but their settings are disabled. You must configure the plugins to use them.

Verify the relative path

Verify that the relative path for the plugin is correct.

Task

1. Open the plugin settings:
   a. In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.
   b. Select the appropriate plugin.
   c. Right-click the plugin and select **Properties**.
2. In the Relative Path field, verify the path:
   - ICAP plugin — `McAfee\ICAPFilter.dll`
   - Proxy chaining plugin — `McAfee\ChainFilter.dll`

   The relative path is set during installation. The path must be relative to the Microsoft ISA Server root path for the plugin to function.

No changes are needed for the Enable this filter checkbox. This checkbox is already selected because the plugins are enabled by default.

3 ICAP plugin

You can use the ICAP plugin to integrate your Microsoft ISA Server with a McAfee Web Gateway or McAfee Data Loss Prevention appliance. This section contains instructions specific for each McAfee product. Be sure to follow the instructions appropriate for your environment.

Contents

About the ICAP plugin

Use the ICAP plugin to redirect unencrypted (HTTP) web traffic from the Microsoft ISA Server to the McAfee Web Gateway appliance or McAfee DLP for content filtering.

- **McAfee Web Gateway** — Use the ICAP plugin to redirect either or both inbound (RESPMOD) and outbound (REQMOD) unencrypted (HTTP) web traffic from the Microsoft ISA Server to the ICAP server on the McAfee Web Gateway appliance. When traffic reaches the ICAP server on the McAfee Web Gateway appliance, it takes action on the traffic (by modifying the request) according to policies and rules set up on the appliance. The McAfee Web Gateway appliance then sends a response back to the Microsoft ISA Server, which delivers the response to the user. If the response is to block the web traffic, the user is blocked from access to that particular website or webpage. If the response is to allow the web traffic, the user is allowed to access that particular website or webpage.
- **McAfee DLP** — Use the ICAP plugin to redirect outbound (REQMOD) unencrypted (HTTP) web traffic from the Microsoft ISA Server to the ICAP server on the McAfee DLP appliance. When traffic reaches the ICAP server on the McAfee DLP appliance, it is analyzed according to policies and rules set up in the McAfee DLP applaince. The McAfee DLP appliance then sends a response back to the Microsoft ISA Server, which delivers the response to the user. If the response is to block the web traffic, the user is blocked from access to that particular website or webpage. If the response is to allow the web traffic, the user is allowed to access that particular website or webpage. For more information about McAfee DLP, see the product documentation.

The ICAP plugin has been successfully tested on standalone and array-configured Microsoft ISA Servers.

See also

REQMOD and RESPMOD on page 12
Statistics for the ICAP plugin on page 22
Introducing McAfee Plugins for Microsoft ISA Server on page 3

REQMOD and RESPMOD

ICAP has two modes: REQMOD (request mode) and RESPMOD (response mode). Each mode scans a web traffic request between the user and the web.

About REQMOD

REQMOD scans the user's web request (outbound traffic) as it travels out to the web.

When using ICAP, the outbound web traffic request arrives at the Microsoft ISA Server where the ICAP plugin redirects it to the McAfee Web Gateway or McAfee DLP appliance. The McAfee Web Gateway or McAfee DLP appliance then filters the request, determines if it is allowed or blocked, and sends that allowed or blocked response back to the Microsoft ISA Server.

If the request is blocked, then the ICAP server on the McAfee Web Gateway or McAfee DLP appliance modifies the request and sends it back to the Microsoft ISA Server. The request is modified with a valid HTTP response, such as the request to a particular URL is not allowed. The Microsoft ISA Server then sends the block response to the user. The actual block response is based on policies and rules set up in the McAfee Web Gateway or McAfee DLP appliance.

If the request is allowed, then the Microsoft ISA Server sends the request out to the web to get the content. At this point, RESPMOD starts.

About RESPMOD

RESPMOD scans the response to the user (inbound traffic) from the web.

After REQMOD is done and the request is allowed, then the web sends back the content. The response arrives at the Microsoft ISA Server where the ICAP plugin redirects it to the McAfee Web Gateway appliance. The McAfee Web Gateway appliance filters the content and takes action based on polices and rules you have set up.

If the response is allowed, it is sent back to the Microsoft ISA Server, which then delivers the web content to the user.

If the response is blocked, then the ICAP server on the McAfee Web Gateway appliance modifies the request and sends it back to the Microsoft ISA Server. The request is modified with a valid HTTP response, such as the request to a particular URL is not allowed. The Microsoft ISA Server then sends the block response to the user. The actual block response is based on policies and rules set up in the McAfee Web Gateway appliance.

Depending on your McAfee Web Gateway policies, you might scan both incoming and outgoing requests, or only one of them.

See also

About the ICAP plugin on page 11

Configure the ICAP plugin for McAfee Web Gateway 6.x appliance

Configure the ICAP plugin for use with a McAfee Web Gateway 6.x appliance.

Configure the following for the ICAP plugin with a McAfee Web Gateway 6.x appliance.

The ICAP plugin is enabled by default.

1 Enable and configure the REQMOD and RESPMOD server settings on the plugin.

2 (Optional) Configure REQMOD and RESPMOD logging on the McAfee Web Gateway 6.x appliance.

3 Enable logging and debugging on the plugin.

4 Enter hosts that you want to bypass.

5 Configure the ICAP(S) Server on the McAfee Web Gateway 6.x appliance.

Enable and configure REQMOD and RESPMOD server settings

Configure REQMOD and RESPMOD servers settings on the ICAP plugin.

Both REQMOD and RESPMOD are disabled by default, you must configure these settings on the plugin if you want to use them.

REQMOD is required in order to use the following McAfee Web Gateway features:

- All URL filters (URL Filter Database, Extended List, Shell Expression)
- Some of the privacy filters (Referer Filter, Cookie Filter)

RESPMOD is required in order to use the following McAfee Web Gateway features:

- Anti-Malware
- Content Security filters
- Some of the privacy filters (Web Bug Filter, Prefix Filter, Cookie Filter)

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 Configure the REQMOD or RESPMOD settings.

   This setting on the plugin handles only HTTP requests; all HTTPS traffic is ignored.

   - **Enable** — Select this checkbox to filter outgoing HTTP requests.
   - **Bypass on failure** — Select this checkbox to continue allowing user HTTP requests when the McAfee Web Gateway ICAP server is unable to respond.
   - **Servers (one per line)** — Enter a McAfee Web Gateway appliance host name or IP address, one per line, and delete the prepopulated examples. The ICAP plugin redirects HTTP requests to the McAfee Web Gateway appliances listed in this field. Use the following example as guidance when entering a McAfee Web Gateway appliance host name or IP address:
     - icap://<ip address>:1344/wwreqmod
     - icap://<ip address>:1344/wwrespmod

   

   For array environments, the ICAP server URI entered on one member is shared across all members of an array. If one server is unavailable, the next server is tried until an available server is found.

Configure REQMOD and RESPMOD logging on the McAfee Web Gateway 6.x appliance

Enable REQMOD and RESPMOD logging on the McAfee Web Gateway 6.x appliance when you want a record of what traffic is being filtered.

Task

1 Log on to the McAfee Web Gateway appliance's user interface.

2 Select **Reporting** | **Log File Management** | **Activate Log Files**.

3 Select the **HTTP Access Denied Log** checkbox for:

- **Web Requests REQMOD**
- **Web Downloads RESPMOD**

Enable category and debug logging McAfee Web Gateway 6.x appliance

Configure the ICAP plugin to log category information to the Microsoft ISA Server access log, and log plugin connection debugging information.

Adding category information to the Microsoft ISA Server access allows you to use the log data to run reports about your organization's web traffic using McAfee Web Reporter. For more information, see the McAfee Web Reporter product documentation.

Task

1 Open the plugin settings:

a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

b Select the appropriate plugin.

c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 To log category information, select the **Modify 'cs-uri' field** checkbox and configure the necessary option or rules on your appliance.

This option writes category information to the Microsoft ISA Server access log file. If you enable this option, the category information is appended to the Microsoft ISA Server access log file's cs-uri field.

Example modified cs-uri Microsoft ISA Server log field:

```
x-attr:"bu" x-filter-result:0 http://www.example.com
```

where:

`x-attr:”bu”` = category information

`“bu”` = the category (which is Business)

`x-filter-result:0` = the action taken

`0` = there was no action taken (such as block, warn, or allow)

4 To log connection debug information, select the **Trace Connections** checkbox. Information about what the ICAP plugin receives from the McAfee Web Gateway appliance and returns to the Microsoft ISA Server is logged to a file stored in the specified directory.

- This setting is not shared across an array. Configure this option on each member of the array when you want debugging enabled on the other members.
- Enabling debugging on the plugin does not enable debugging on the ICAP server.

Logs stored in the directory are not automatically deleted. Each time the Trace connections option is enabled (either through a service restart or disabling and then re-enabling it), a new file with a GMT time stamp is created.

Configure host bypass

Configure the host names, IP addresses, or domain names that will bypass filtering so that requests to those names and addresses are always allowed.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Bypass List** tab.

3 In the **Hosts to bypass** field, enter one host per line.

   Enter an exact host name, IP address, or domain name using the examples below as guidelines. Wildcards are not valid (entering **example.com* or *example.com* does not include all *example.com* domains).

   Examples:

   - www.example.com
   - mail.example.com
   - 192.168.254.22
   - FD4A:A1B2:C3D4:0:0:0:0:E5F6

4 Click **OK** to save the configuration.

Configure ICAP(S) server on McAfee Web Gateway 6.x appliance

Configure the ICAP(S) Server to allow the McAfee Web Gateway 6.x appliance to accept incoming ICAP connections from the ICAP plugin and to return category information and header values with all ICAP responses. The ICAP(S) Server is enabled by default.

Before you begin

You must have already enabled and configured the ICAP plugin.

Task

1 Log on to the McAfee Web Gateway 6.x appliance's user interface.

2 Select **Proxies** | **ICAP(S) Server** | **Server Settings**.

3 Select one of the following:

- **Send all categories to the ICAP client**
- **Send only the blocked categories to the ICAP client**

4 Select the **Send range of values of the 'X-Attribute' header in OPTIONS response** checkbox.

5 Click **Apply Changes**.

The McAfee Web Gateway 6.x ICAP(S) Server is configured to send category information and 'X-Attribute' header range values with all ICAP responses.

Configure the ICAP plugin for a McAfee Web Gateway 7.x appliance

The tasks in this section are specifically for configuring the ICAP plugin for use with a McAfee Web Gateway 7.x appliance.

Configure the following for the ICAP plugin with a McAfee Web Gateway 7.x appliance.

The ICAP plugin is enabled by default.

1 Configure REQMOD and RESPMOD server settings on the plugin.

2 Enable logging and debugging on the plugin.

3 Enter hosts that you want to bypass.

4 Enable the ICAP server on the McAfee Web Gateway 7.x appliance.

REQMOD and RESMOD logging is enabled by default on the McAfee Web Gateway 7.x appliance.

Enable and configure REQMOD and RESPMOD server settings

Configure REQMOD and RESPMOD servers settings on the ICAP plugin.

Both REQMOD and RESPMOD are disabled by default, you must configure these settings on the plugin if you want to use them.

REQMOD is required in order to use the following McAfee Web Gateway features:

- All URL filters (URL Filter Database, Extended List, Shell Expression)
- Some of the privacy filters (Referer Filter, Cookie Filter)

RESPMOD is required in order to use the following McAfee Web Gateway features:

- Anti-Malware
- Content Security filters
- Some of the privacy filters (Web Bug Filter, Prefix Filter, Cookie Filter)

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 Configure the REQMOD or RESPMOD settings.

   This setting on the plugin handles only HTTP requests; all HTTPS traffic is ignored.

   - **Enable** — Select this checkbox to filter outgoing HTTP requests.
   - **Bypass on failure** — Select this checkbox to continue allowing user HTTP requests when the McAfee Web Gateway ICAP server is unable to respond.
   - **Servers (one per line)** — Enter a McAfee Web Gateway appliance host name or IP address, one per line, and delete the prepopulated examples. The ICAP plugin redirects HTTP requests to the McAfee Web Gateway appliances listed in this field. Use the following example as guidance when entering a McAfee Web Gateway appliance host name or IP address:
     - icap://<ip address>:1344/wwreqmod
     - icap://<ip address>:1344/wwrespmod

   

   For array environments, the ICAP server URI entered on one member is shared across all members of an array. If one server is unavailable, the next server is tried until an available server is found.

Enable category and debug logging McAfee Web Gateway 7.x appliance

Configure the ICAP plugin to log category information to the Microsoft ISA Server access log, and log plugin connection debugging information.

Adding category information to the Microsoft ISA Server access allows you to use the log data to run reports about your organization's web traffic using McAfee Web Reporter. For more information, see the McAfee Web Reporter product documentation.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 To log category information, select the **Modify 'cs-uri' field** checkbox and configure the necessary option or rules on your appliance.

This option is available for backwards compatibility with McAfee Web Gateway 6.x appliances when the ICAP(S) Server is configured. If you want to use this option with a McAfee Web Gateway 7.x appliance, you need to configure a rule that adds outgoing ICAP headers with category and block information for a policy. To configure rules and policies, see the McAfee Web Gateway product documentation for your appliance.

Example modified cs-uri Microsoft ISA Server log field:

```
x-attr:"bu" x-filter-result:0 http://www.example.com
```

where:

`x-attr:”bu”` = category information

`“bu”` = the category (which is Business)

`x-filter-result:0` = the action taken

`0` = there was no action taken (such as block, warn, or allow)

4 To log connection debug information, select the **Trace Connections** checkbox. Information about what the ICAP plugin receives from the McAfee Web Gateway appliance and returns to the Microsoft ISA Server is logged to a file stored in the specified directory.

- This setting is not shared across an array. Configure this option on each member of the array when you want debugging enabled on the other members.
- Enabling debugging on the plugin does not enable debugging on the ICAP server.

Logs stored in the directory are not automatically deleted. Each time the Trace connections option is enabled (either through a service restart or disabling and then re-enabling it), a new file with a GMT time stamp is created.

Configure host bypass

Configure the host names, IP addresses, or domain names that will bypass filtering so that requests to those names and addresses are always allowed.

Task

1 Open the plugin settings:

a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

b Select the appropriate plugin.

c Right-click the plugin and select **Properties**.

2 Click the **Bypass List** tab.

3 In the **Hosts to bypass** field, enter one host per line.

Enter an exact host name, IP address, or domain name using the examples below as guidelines. Wildcards are not valid (entering **example.com* or *example.com* does not include all *example.com* domains).

Examples:

- www.example.com
- mail.example.com
- 192.168.254.22
- FD4A:A1B2:C3D4:0:0:0:0:E5F6

4 Click **OK** to save the configuration.

Enable the ICAP server on a McAfee Web Gateway 7.x appliance

Enable the ICAP server to allow the McAfee Web Gateway appliance to accept incoming ICAP connections from the ICAP plugin.

Before you begin

You must have already enabled and configured the ICAP plugin.

After the ICAP server is enabled, no further configuration is required.

Task

1 Log on to the McAfee Web Gateway appliance's user interface.

2 Select **Configuration** | **Proxies (HTTP(S), FTP, ICAP and IM)**.

3 In the ICAP server section, select **Enable ICAP Server** (if it is not already selected).

If you want to use the Modify 'cs-uri' field option, you must also configure a rule to add outgoing ICAP headers with category or block information for a policy. To configure rules and policies, see the McAfee Web Gateway product documentation for your appliance.

4 Click **Save Changes**.

The McAfee Web Gateway ICAP Server is enabled.

Configure the ICAP plugin for McAfee DLP

The tasks in this section are specifically for configuring the ICAP plugin for use with McAfee DLP.

Configure the following for the ICAP plugin with a McAfee DLP appliance.

The ICAP plugin is enabled by default.

1 Enable and configure REQMOD servers settings (RESPMOD is not available for this configuration).

2 Enable debug logging (logging category information is not available for this configuration).

3 Enter domains to bypass.

4 Configure the ICAP server on the McAfee DLP appliance.

After you complete the configuration steps, traffic is filtered through the rules and policies that are set up on your McAfee DLP appliance.

Enable and configure REQMOD settings

Configure the plugin to redirect outbound traffic (REQMOD) to a McAfee DLP appliance.

REQMOD is disabled by default, you must configure this setting on the plugin if you want to use it.

Do not enable or try to use the RESPMOD (inbound requests) settings as this option has no functionality when using the ICAP plugin with a McAfee DLP appliance.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 Enable and configure the REQMOD settings.

   This setting on the plugin handles only HTTP requests; all HTTPS traffic is ignored.

   - **Enable** — Select this checkbox to filter outgoing HTTP requests and replace the default value with your McAfee DLP appliance ICAP server URI.
   - **Bypass on failure** — Select this checkbox to continue allowing user HTTP requests when the McAfee DLP appliance ICAP server is unable to respond.
   - **Servers (one per line)** — Enter a McAfee DLP host name or IP address, one per line, use the **icap://127.0.0.1:1344/reqmod** prepopulated example as a guideline and then delete it. The ICAP plugin redirects HTTP requests to the McAfee DLP appliances listed in this field.

     For array environments, the ICAP server URI entered on one member is shared across all members of an array. If one server is unavailable, the next server is tried until an available server is found.

Enable debug logging

Log plugin connection debugging information to record information about what the ICAP plugin receives from the client (Microsoft ISA Server) and returns to the client.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 To log connection debug information, select the **Trace Connections** checkbox. Information about what the ICAP plugin receives from the McAfee DLP appliance and returns to the Microsoft ISA Server is logged to a file stored in the specified directory.

- This setting is not shared across an array. Configure this option on each member of the array when you want debugging enabled on the other members.
- Enabling debugging on the plugin does not enable debugging on the ICAP server.

Logs stored in the directory are not automatically deleted. Each time the Trace connections option is enabled (either through a service restart or disabling and then re-enabling it), a new file with a GMT time stamp is created.

Configure host bypass

Configure the host names, IP addresses, or domain names that will bypass filtering so that requests to those names and addresses are always allowed.

Task

1 Open the plugin settings:

a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

b Select the appropriate plugin.

c Right-click the plugin and select **Properties**.

2 Click the **Bypass List** tab.

3 In the **Hosts to bypass** field, enter one host per line.

Enter an exact host name, IP address, or domain name using the examples below as guidelines. Wildcards are not valid (entering **example.com* or *example.com* does not include all *example.com* domains).

Examples:

- www.example.com
- mail.example.com
- 192.168.254.22
- FD4A:A1B2:C3D4:0:0:0:0:E5F6

4 Click **OK** to save the configuration.

Configure the ICAP server on the McAfee DLP appliance

You must configure the ICAP server on the McAfee DLP appliance when you want to use the ICAP plugin.

Contact McAfee DLP support for more information about configuring the ICAP server on the McAfee DLP appliance.

Statistics for the ICAP plugin

The ICAP plugin allows you to view and reset statistics about the plugin.

Statistics on the Statistics tab display information for REQMOD and RESPMOD requests that have been issued and for connections to the ICAP server. In an array environment, the statistics data relates only to the plugin on the member you are accessing.

The following table provides a description for each statistic.

Table 3-1 Statistics descriptions

Name	Description
REQUESTS — Number of REQMOD and RESPMOD requests made	
• **ICAP 200s** • **ICAP 204s** • **ICAP 204s (after preview)** • **ICAP 400s**	Number of ICAP status code responses returned to the plugin
Failed	Number of times an ICAP request could not be completed
Total	Total number of requests
CONNECTIONS — Number of connections to the ICAP servers	
Open	Number of connections that are available for use
Active	Number of connections that are currently in use
Peak	Highest number of active connections recorded

See also

About the ICAP plugin on page 11

Reset statistics

Use this task to reset statistics.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Selct the **Statistics** tab.

3 Click **Reset** to reset statistics.

Statistics information is automatically updated every few seconds.

4 Proxy chaining plugin

You can use the proxy chaining plugin to integrate McAfee Web Gateway or McAfee SaaS Web Protection into your Microsoft ISA Server-based network environment. This section contains instructions specific for each McAfee product. Be sure to follow the instructions appropriate for your setup.

Contents

About the proxy chaining plugin

You can use the proxy chaining plugin with a McAfee Web Gateway appliance as an upstream proxy server for content and URL filtering, or with the McAfee SaaS Web Protection service for URL filtering.

- McAfee Web Gateway — Use the McAfee Web Gateway appliance as an upstream proxy server in your proxy chain environment to analyze web traffic and apply filters to URLs or content, which adds security against web-based threats. When you use the McAfee Web Gateway appliance as an upstream proxy, the proxy chaining plugin forwards web traffic requests that are passing through your network to the McAfee Web Gateway appliance. When the web traffic reaches the appliance, policies you have set up are applied to the requests and then the URLs or content is either allowed or blocked.
- McAfee SaaS Web Protection — Use the McAfee SaaS Web Protection service as an upstream proxy server in your proxy chain environment to analyze URLs in web traffic requests. The proxy chaining plugin forwards web traffic requests to the the McAfee SaaS Web Protection service, where the URLs are identified and either allowed or blocked according to the policies and rules you have set up.

The McAfee Web Gateway appliance or McAfee SaaS Web Protection service adds security for web traffic, and the Microsoft ISA Server handles the remaining network traffic.

If you have caching enabled on the Microsoft ISA Server and user-based policies set up on the McAfee Web Gateway appliance or the McAfee SaaS Web Protection service, all requests might not be forwarded for additional filtering. Because of this, when you enable user-based policies on the McAfee Web Gateway appliance or McAfee SaaS Web Protection service, you should disable caching on the Microsoft ISA Server.

See also

Introducing McAfee Plugins for Microsoft ISA Server on page 3

Configure the proxy chaining plugin for a McAfee Web Gateway appliance

Configure the outbound headers so that each outbound traffic request includes user, group, and IP address information. Configure outbound header settings when using the proxy chaining plugin with a McAfee Web Gateway 6.x or 7.x appliance.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Click the **Config** tab.

3 Select or clear the options for McAfee Web Gateway outbound headers and verify or enter the header name. By default, McAfee Web Gateway header names are entered.

- **Include User Header** — Forwards the user name of the user making the request
- **Include Group Header** — Forwards the groups that the user making the request belongs to
- **Include Forwarded For Header** — Forwards the IP address of the machine making the request

The header names must match the web mappings header names configured on your McAfee Web Gateway appliance

4 Click **OK** to save the changes.

After the proxy chaining plugin is functional, you must configure the Microsoft ISA Server for proxy chaining.

Configure the proxy chaining plugin for McAfee SaaS Web Protection

Configure the proxy chaining plugin to authenticate with McAfee SaaS Web Protection.

Use the McAfee SaaS Web Protection configuration in the plugin to enable access to McAfee SaaS Web Protection.

The outbound header settings apply only to the McAfee Web Gateway appliance. The header settings do not apply when using the plugin with McAfee SaaS Web Protection. For more information about McAfee SaaS Web Protection, see the product documentation.

Task

1 Open the plugin settings:

   a In the Microsoft ISA Server management console, select **Arrays** | **[your array]** | **Configuration** | **Add-ins**, then click the **Web Filters** tab.

   b Select the appropriate plugin.

   c Right-click the plugin and select **Properties**.

2 Select the **Config** tab.

3 Select the **Use Web Protection Service** checkbox to enable this option.

4 Enter the McAfee SaaS Web Protection customer ID and password.

5 Click **OK** to save the changes.

After you complete the configuration steps, traffic is filtered through the rules and policies that are set up in McAfee SaaS Web Protection.

Configure proxy chaining rules on the Microsoft ISA Server

Configure proxy chaining on the Microsoft ISA Server.

Task

1 Open the Microsoft ISA Server and create the web chaining rules you need.

2 Follow these guidelines when creating the web chaining rules:

- Configure the request action to redirect to a specified upstream server.

  Do not enable delegation of basic authentication credentials.

- Configure the primary route:
  - **Server** — Enter the McAfee Web Gateway appliance or McAfee SaaS Web Protection service IP address.
  - **Port** — Enter the HTTP port used by the McAfee Web Gateway appliance (default is 9090) or McAfee SaaS Web Protection service (default is 8080).
  - **SSL Port** — Enter the HTTPS port used by the McAfee Web Gateway appliance (default is 443) or McAfee SaaS Web Protection service (default is 8080).

Index

S

T

U

W