Product Guide

Revision A

McAfee Web Gateway 7.2

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

This Product Guide describes the features and capabilities of McAfee® Web Gateway version 7.2, providing an overview of the product, as well as detailed instructions on how to set it up, configure, and maintain it.

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.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

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.
ℹ	**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.

The McAfee Web Gateway appliance is introduced with overviews of main functions, deployment options, system architecture, and administrator activities.

This is followed by an explanation of how to setup the appliance and complete first steps up to the point where you configure proxy, authentication, and web filtering functions.

Configuration of these main functions is explained in separate chapters.

It is also explained how to configure functions of the appliance system, such as domain name services, port forwarding, or static routes, and how to set up an appliance as a node in a Central Management configuration.

Chapters on monitoring and troubleshooting are provided at the end of the guide.

An appendix contains lists of important configuration elements, such as actions, events, properties, and others.

Find 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 Introduction

The McAfee® Web Gateway appliance ensures comprehensive web security for your network.

It protects your network against threats arising from the web, such as viruses and other malware, inappropriate content, data leaks, and related issues. It also ensures regulatory compliance and a productive work environment.

Contents

Filtering web traffic

The appliance is installed as a gateway that connects your network to the web and filters the traffic that goes out and comes in.

Following the implemented web security rules, it filters the requests that users send to the web from within your network and the responses that are sent back from the web.

Embedded objects sent with requests or responses are also filtered.

Malicious and inappropriate content is blocked, while useful matter is allowed to pass through.

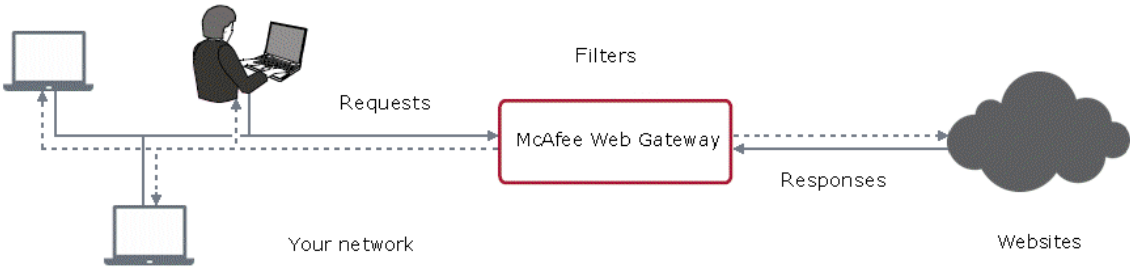


Figure 1-1 Filtering web traffic

Main functions of the appliance

Filtering web traffic is a complex process. The main functions of the appliance contribute to it in different ways.

Filtering web objects

Special anti-virus and anti-malware functions on the appliance scan and filter web traffic and block web objects if they are infected.

Other functions filter requested URLs, using information from the Global Threat Intelligence™ system, or perform media type and application filtering.

They are supported by functions that do not filter themselves, but complete such jobs as counting user requests or indicating the progress made in downloading web objects.

Filtering users

Authentication functions of the appliance filter users, using information from internal and external databases and methods such as NTLM, LDAP, RADIUS, Kerberos, and others.

In addition to filtering normal users, the appliance also gives you control over administrator rights and responsibilities.

Intercepting web traffic

This is a prerequisite for any filtering of web objects or users. It is achieved by the proxy functions of the appliance, using different network protocols, such as HTTP, HTTPS, FTP, Yahoo, ICQ, Windows Live Messenger, XMPP, and others.

The appliance can run in explicit proxy mode or in transparent bridge or router mode.

Monitoring the filtering process

The monitoring functions of the appliance provide a continuous overview of the filtering process.

They include a dashboard, which displays information on alerts, web usage, filtering activities, and system behavior. Logging and tracing functions are also available, as well as options to forward data to an McAfee ePO server or do event monitoring with an SNMP agent.

Main components of the appliance

The McAfee Web Gateway appliance uses several subsystems to provide filtering and other functions, based on its operating system.

Appliance subsystems

The subsystems of the appliance and their modules do the following:

- **Core subsystem** — Provides a proxy module for intercepting web traffic and a rule module for processing the filtering rules that make up your web security policy.

  This subsystem furthermore provides the modules (also known as engines) that complete special jobs for the filtering rules and can be configured by you, for example, the Anti-Malware module, the URL Filter module, or the Authentication module.

  A flow manager module ensures efficient cooperation between the modules.

- **Coordinator subsystem** — Stores all configuration data processed on the appliance

  This subsystem also provides update and Central Management functions.

- **Configurator subsystem** — Provides the user interface (internal subsystem name is *Konfigurator*)

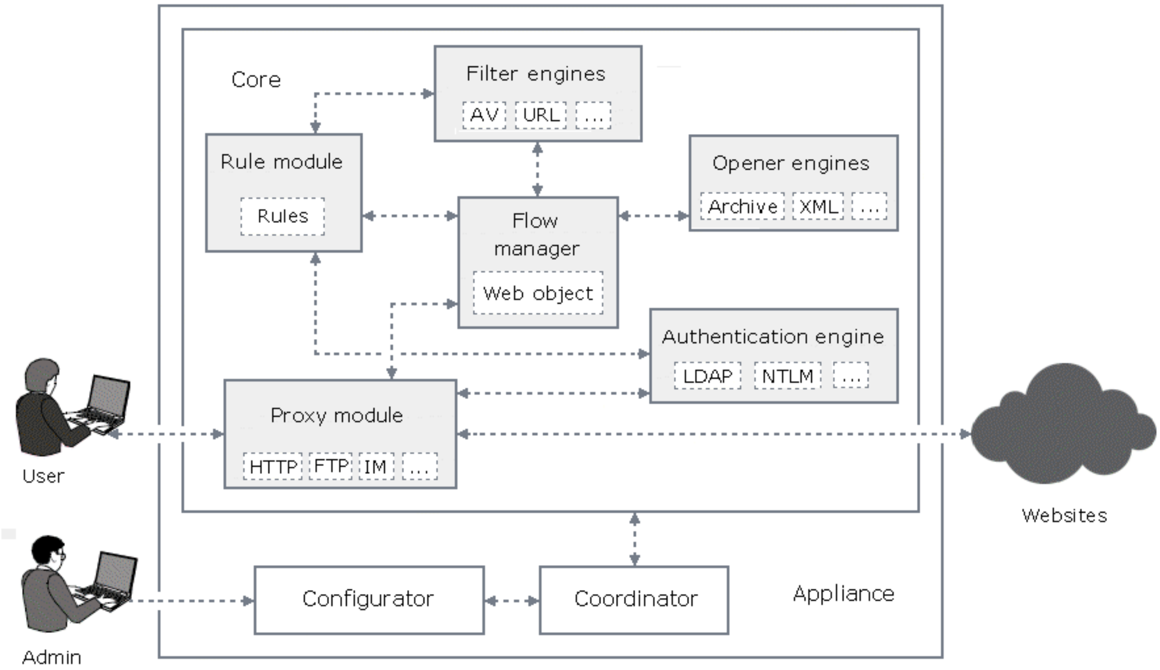


Figure 1-2 Appllance subsystems and modules

Operating system

The subsystems of the appliance rely on the functions of its operating system, which is MLOS (McAfee Linux Operating System) version 1.0.

The operating system provides functions for executing the actions that the filtering rules trigger, file and network reading and writing, and access control.

A configuration daemon (sysconfd daemon) implements changed configuration settings in the operating system.

Deployment of the appliance

Before you set up the McAfee Web Gateway appliance, consider how you want to use it. You can run it on different platforms and configure different modes of network integration. You can also set up and administer multiple appliances as nodes in a Central Management configuration.

Platform

You can run the appliance on different platforms.

- **Hardware-based appliance** — On a physical hardware platform
- **Virtual appliance** — On a virtual machine

Network integration

In your network, the appliance can intercept, filter, and transmit web traffic in different modes.

- **Explicit proxy mode** — The clients that the appliance communicates with are aware of it. You must configure them "explicitly" to direct their traffic to the appliance.
- **Transparent modes** — The clients are not aware of the appliance.
  - **Transparent bridge** — The appliance acts as an "invisible" bridge between its clients and the web. You need not configure the clients for this.
  - **Transparent router** — The appliance routes traffic according to a routing table, which you need to fill out.

Administration and updates

You can administer the appliance and have updates distributed in different ways.

- **Standalone** — Administer the appliance separately and let it not receive updates from other appliances.
- **Central Management** — Set up the appliance as a node in a complex configuration and administer other nodes on its user interface, including the distribution of updates.

  You can then administer the appliance on other nodes and let it receive updates from them.

High-level administration activities

Administering the appliance includes different activities, depending on the requirements of your network. The following are recommended high-level administration activities.

Task

1. Perform the initial setup.

   The setup procedure includes the initial configuration of system parameters, such as host name and IP address, implementing an initial system of filtering rules, and licensing.

   Two wizards are available in this phase: one for the initial configuration, another for the filtering rules.

2 Configure the proxy functions.

After the initial setup, explicit proxy mode and the HTTP protocol are preconfigured on the appliance.

You can modify this setup and also configure other network components that the appliance communicates with.

3 Consider implementing authentication.

Authentication is not implemented on the appliance by default.

If you want to implement it, you can choose from a number of different authentication methods, including NTML, LDAP, Kerberos, and others.

4 Configure web filtering.

You can review the rules that have been implemented during the initial setup for virus and malware filtering, URL filtering, media type filtering, and other filtering-related processes.

You can finetune these rules and adapt them to the needs of your network.

Working on the filtering rules includes maintaining the lists that the rules use and configuring the settings for rule actions and the modules that are involved in the filtering process.

5 Monitor the appliance behavior.

When you have configured the appliance according to your requirements, you can monitor it to see how it performs the filtering process.

You can also monitor system functions, such as CPU and memory usage, number of active connections, and others.

For more information on these activities, see the sections that deal with them, for example, under *Setup*, *Authentication*, or *Web filtering*.

2 Setup

To set up the appliance you need to complete several activities, such as checking your installation materials, working with the installation menu, and logging on to the user interface.

The setup procedure differs according to the platform that you install the appliance software on and the way the software is provided.

When the installation is completed and you log on to the user interface for the first time, you also need to implement an initial system of web security rules and import a license.

Contents

Before you begin

Before you begin to set up the appliance, check whether the requirements for this task are met.

What is required depends on how you want to set up the appliance. You can set it up as:

- **Hardware-based appliance**

  The appliance software is then available in the following ways:

  - **Pre-installed software** — When you purchase a new hardware platform for McAfee Web Gateway, the appliance software is pre-installed on it.

  - **Downloaded software** — If you do not want to use the pre-installed software, you can download a USB version of the software from the McAfee Content & Cloud Security Portal and install it on your hardware platform.

- **Virtual appliance**

  To set up a virtual appliance, you need to download an ISO image of the appliance software and install it on a virtual machine.

Requirements for setting up a hardware-based appliance

When you have purchased a new hardware platform, the following is required for the setup:

- Items that were shipped to you:
    - Hardware platform (models vary) with appliance software
    - Power cord
    - Network cables
    - USB-PS/2 adapter cable (if you use a PS/2 keyboard for the initial configuration)
- Items that you must provide:
    - Standard VGA monitor and PS/2 keyboard
      or Serial console
    - Administration system with:
        - Windows or Linux operating system
        - Java Runtime Environment (JRE) version 1.6 or later
        - Microsoft Internet Explorer version 6.0 or later
          or Mozilla Firefox version 2.0 or later
    - Network cables

Requirements for setting up a virtual appliance

To set up a virtual appliance the following is required:

- One of the following VMware types:
    - VMware ESX
    - VMware ESXi

  VMware workstation version 5.5 or later is not supported, but can be used for testing purposes.
- Virtual machine host system with the following specifications:
    - CPU: 64-bit capable
    - Virtualization extension: VT-x/AMD-V
- Virtual machine with the following specifications:
    - Memory: 4 GB
    - Hard-disk space: 200 GB
    - CPU cores: 2 (minimum)

High-level steps for setting up the appliance

To set up the appliance complete the following high-level steps.

Task

1. Make sure the requirements for the setup are met.
   - If you are setting up a new hardware-based appliance:
     - Check the hardware platform and accessories that have been delivered to you.
     - Check whether you have the materials available that you need to provide for the setup, such as a monitor, keyboard, and other items.
   - If you are setting up a virtual appliance, check whether you have the appropriate VM equipment.
2. Review the default initial configuration settings.

   If these settings do not suit the requirements of your network, you can use an option of the installation menu to configure your own settings.
3. Install the appliance software.
   - If you are setting up a hardware-based appliance with pre-installed software:
     - Connect and turn on the appliance.
     - Use one of the options on the installation menu to complete the installation.
   - If you are setting up a hardware-based appliance with downloaded USB software:
     - Download the USB software and copy it to a USB drive.
     - Connect the appliance, insert the USB drive, and turn on the appliance.
     - Use the Boot Manager to install the software.
   - If you are setting up a virtual appliance:
     - Download an ISO image and insert it into the host system of the virtual machine.
     - Set up a new virtual machine and turn it on.
     - Use one of the options on the installation menu to install the software.
4. Log on to the user interface.
5. Implement an initial system of web security rules.
6. Import a license.

Default initial configuration settings

You can set up the appliance using default settings for the initial configuration or implement your own initial settings.

The following table shows the settings that are used by default.

Table 2-1 Default initial configuration settings

Parameter	Value
Primary network interface	eth0
Autoconfiguration with DHCP	yes
Host name	mwgappl

Table 2-1 Default initial configuration settings *(continued)*

Parameter	Value
Root password	<none>
Remote root logon with SSH	on
Default gateway	<configured by DHCP>
DNS server	<configured by DHCP>

Set up a hardware-based appliance with pre-installed software

On a newly purchased hardware platform, the appliance software is pre-installed. You need to connect the appliance and work with the installation menu to complete the installation of the appliance software.

Tasks

- *Connect and turn on the appliance* on page 22
  When using a hardware-based appliance with pre-installed software, you begin the installation by connecting and turning on the appliance.
- *Install the appliance software using the installation menu* on page 22
  To complete the installation of pre-installed software on a hardware platform, you work with the installation menu.
- *Implement your own initial configuration settings* on page 24
  You can implement your own initial configuration settings instead of the default settings, using a wizard.

Connect and turn on the appliance

When using a hardware-based appliance with pre-installed software, you begin the installation by connecting and turning on the appliance.

Task

1. Connect the appliance to power and the network.
2. Connect a monitor and keyboard or a serial console to the appliance.
3. Turn on the appliance.

   The installation menu appears.

You can now work with the installation menu to complete the installation of the appliance software.

Install the appliance software using the installation menu

To complete the installation of pre-installed software on a hardware platform, you work with the installation menu.

The installation menu allows you to call a configuration wizard for implementing your own initial configuration settings. You can also choose to set up the appliance in a FIPS-compliant mode.

Task

1. Select an option from the installation menu and press **Enter**.

2. Continue with the installation procedure.

   - If you have selected an option without wizard and not entered the FIPS compliance submenu, confirm when prompted.

     The installation is completed. The appliance runs with default initial configuration settings in a non FIPS-compliant mode.

     You can now log on to the user interface.

   - If you have selected the option for entering the FIPS compliance submenu:

     - Select an option from this menu and press **Enter**.

     - Confirm when prompted.

       The installation is completed. The appliance runs with default initial configuration settings in a FIPS-compliant mode.

       You can now log on to the user interface.

   - If you have selected a wizard mode from the main menu or the submenu, work with the wizard to implement your own initial configuration settings.

Installation menu options

The installation menu provides options for installing the appliance software in different modes.

The following table shows these options.

Table 2-2 Installation menu options

Option	Definition
1 – Serial console **(with configuration wizard)**	System output is displayed on a serial console. When the first part of the installation is over, the appliance restarts and displays a wizard for implementing initial configuration settings.
2 – Video console **(with configuration wizard)**	System output is displayed on a video console. When the first part of the installation is over, the appliance restarts and displays a wizard for implementing the initial configuration settings.
3 – Serial console	System output is displayed on a serial console. When the first part of the installation is over, the appliance restarts and waits for your confirmation to complete the installation.
4 – Video console	System output is displayed on a video console. When the first part of the installation is over, the appliance restarts and waits for your confirmation to complete the installation.

Table 2-2 Installation menu options *(continued)*

Option	Definition
5 – FIPS 140-2 level 2	Opens a submenu for installing the appliance software in a FIPS-compliant mode. • **1 – FIPS 140-2 level 2 (serial)** System output is displayed on a serial console. Installation in this mode disables logon to the appliance using SSH or from a console and implements other features required for FIPS compliance. When the first part of the installation is over, the appliance waits for your confirmation to complete the installation. • **2 – FIPS 140-2 level 2 (configuration wizard – serial)** As submenu option 1, but with wizard When the first part of the installation is over, the appliance restarts and displays a wizard for implementing the initial configuration settings. • **3 – FIPS 140-2 level 2 (enforce self-failed test – serial)** Recovers the appliance when a FIPS self-test has failed after starting submenu option 1 or 2. After the recovery, use one of these two options to repeat the installation. • **4 – FIPS 140-2 level 2 (video)** As submenu option 1, but with output on a video console • **5 – FIPS 140-2 level 2 (configuration wizard – video)** As submenu option 4, but with wizard When the first part of the installation is over, the appliance restarts and displays a wizard for implementing the initial configuration settings. • **6 – FIPS 140-2 level 2 (enforce self-failed test – video)** Recovers the appliance when a FIPS self-test has failed after starting submenu option 4 or 5. After the recovery, use one of these two options to repeat the installation.
9 – Boot from hard disk	The appliance restarts with software that is already installed on a hard disk.

Implement your own initial configuration settings

You can implement your own initial configuration settings instead of the default settings, using a wizard.

The wizard appears when you select an appropriate option from the installation menu.

Task

1 Use the wizard windows to configure the following:

- Primary network interface
- IP address, entered manually or configured dynamically by DHCP
- Host name
- DNS server

2. Review the summary that is displayed after configuring the host name.
   - If you approve of the summary, confirm and configure the remaining settings:
     - Root password

       This option is not available in FIPS-compliant modes.
     - Remote logon with SSH

       This option is not available in FIPS-compliant modes.

     The appliance software is installed with your settings and the IP address is displayed.

     You can now log on to the user interface.
   - If you need to make changes, click **Cancel** and return to step 1.

Set up a hardware-based appliance with downloaded software

When you set up the appliance on a hardware platform, you can install appliance software that you downloaded from the Extranet for McAfee Web Gateway.

You download the software in USB format and work with the boot manager on the hardware platform to install it.

Tasks

- *Download the USB software* on page 25
  You can download different versions of the appliance software in USB format from the Content & Cloud Security Portal.
- *Install the downloaded USB software* on page 26
  To install the downloaded USB software on a hardware-based appliance you connect the appliance and work with the Boot Manager.

Download the USB software

You can download different versions of the appliance software in USB format from the Content & Cloud Security Portal.

Task

1. Use a browser to go to:

   https://contentsecurity.mcafee.com/
2. Submit your user name and password.
3. Beginning on the home page of the McAfee Content & Cloud Security Portal, select **Software** | **McAfee Web Gateway 7** | **Download**.

   A page with software versions in USB and ISO format appears.
4. Click the USB icon for the exact software version you want to download.

   A download window opens.
5. Select the option for storing a file and click **OK**.

   The software is downloaded and stored within your file system.
6. Copy the downloaded software to a USB drive to have it available for installation.

Install the downloaded USB software

To install the downloaded USB software on a hardware-based appliance you connect the appliance and work with the Boot Manager.

Task

1 Connect the appliance to power and the network.

2 Connect a monitor and keyboard or a serial console to the appliance.

3 Insert the USB drive with the downloaded software.

4 Turn on the appliance.

   The installation begins.

5 During the initial phase, select the installation device:

   - If your appliance hardware model is McAfee Web Gateway 4500B, 5000B, or 5500B:
     - Press **F6** to enter the Boot Manager.
     - Select **USB Drive**.

     The installation is completed.
   - If your model is McAfee Web Gateway 4000B:
     - Press **F2** to enter the BIOS setup menu.
     - Select **Boot Options** and click **Hard Disk Order**.
     - Select the option that assigns the USB drive the highest priority.
     - Select the **Exit** tab.
     - Select **Discard Changes**.

       ℹ Do not use the **Discard Changes and Exit** option here.
     - Select **Boot Manager** and click **USB Drive**.

     The installation is completed.
   - If your model is not one of those specified:
     - Press **F11** to enter the Boot Manager.
     - Select **USB Drive**.

     The installation is completed.

You can now log on to the user interface.

Set up a virtual appliance

To set up a virtual appliance you download appliance software from the Content & Cloud Security Portal and install it on a virtual machine.

You download the software in ISO format and work with the installation menu to install it.

Tasks

- *Download an ISO image* on page 27
  You can download different versions of the appliance software as ISO images from the Content & Cloud Security Portal.
- *Install a downloaded ISO image* on page 27
  To install a downloaded ISO image on a virtual appliance, you set up a virtual machine and work with the installation menu.

Download an ISO image

You can download different versions of the appliance software as ISO images from the Content & Cloud Security Portal.

Task

1. Use a browser to go to:

   https://contentsecurity.mcafee.com

2. Submit your user name and password.

3. Beginning on the home page of the Content & Cloud Security Portal, select **Software** | **McAfee Web Gateway 7** | **Download**.

   A page with software versions in USB and ISO format appears.

4. Click the ISO icon for the exact software version you want to download.

   A download window opens.

5. Select the option for storing a file and click **OK**.

   The software is downloaded and stored within your file system.

6. Burn the ISO image onto a CD to have it available for installation.

Install a downloaded ISO image

To install a downloaded ISO image on a virtual appliance, you set up a virtual machine and work with the installation menu.

Task

1. Insert the image into the CD drive of the host system for your virtual machine.

2. Start your VMware and configure settings for a new virtual machine.

3. Turn on the new virtual machine.

   The installation menu appears.

You can now select an installation mode from the menu and install the appliance software.

This is done in the same way as for the pre-installed software on a hardware platform.

You can also select a menu option that allows you to work with a wizard and implement your own initial configuration settings.

Virtual machine settings

When setting up a virtual appliance, you need to configure settings for the virtual machine you want to use as the platform for the appliance software.

The procedures for setting up a virtual machine differ for each VMware type. Make sure you configure the settings listed in the following table.

> For parameters that are not listed, use the default values given in the procedures. Parameter names can also differ with each procedure.

Table 2-3 Virtual machine settings

Option	Definition
Configuration type	Typical | Advanced (recommended for virtual appliance setup)
Installation mode	Install from disk | ISO image (required for virtual appliance setup) | Install later
Operating system	Linux (64 bit) version 2.6
Memory	4 GB (recommended)
Hard-disk space	200 GB (recommended)
Number of processors	1 | 2 (minimum requirement) | 4 | ... The number of processors provided for selection depends on the equipment of the host system that is used for setting up the virtual appliance.
Network connection mode	Bridged (recommended) | NAT | ...
CD/DVD drive with assigned ISO image	<drive name>/<name of the ISO image>
SCSI controller (for some ESX versions)	BusLogic Controller (recommended) | LSI Logic Controller

Log on to the user interface

You log on to the user interface of the appliance using a browser on an administration system.

Task

1. Open the browser and go to *http://<IP address>:4711* or *https://<IP address>:4712*, using the IP address configured during the initial configuration.

   Under HTTPS, accept the self-signed certificate that appears.

   A logon window opens.

2. Enter `admin` as the user name and `webgateway` as the password.

After logging on for the first time, you need to implement an initial system of web security rules and import a license.

> While logged on, you should not use your browser to log on to the same appliance again.

Implement an initial system of web security rules

When setting up the appliance, you also implement an initial system of web security rules for your network.

To implement an initial system of web security rules, the Policy Creation Wizard is provided. It appears when you log on to the user interface for the first time after installing the appliance software.

The wizard allows you to make selections for implementing a system. You can also choose not to make any selections and implement the default system.

Task

1. In the wizard window, review the options for organization, location, and level of permission or restriction, upon which a system of rules can be built.
2. Implement an initial system of rules in one of the following two ways:
   - If you want to implement a system based on the provided options:
     - Select values according to your organization, location, and the level of permission or restriction you consider appropriate.
     - Click **OK**.

       A system of web security rules is implemented accordingly.
   - Otherwise click **Default**.

     The default system of web security rules is implemented.

You can now import a license.

After this, you can work with the implemented system of web security rules.

For example, the system provides rules with whitelists and blocking lists that are initially empty. If you want to use these lists for your web security policy, you need to fill the entries.

Import a license

When you are setting up the appliance, you also need to import a license.

The import is done after logging on to the user interface for the first time when you have completed working with the policy creation wizard.

Task

1. On the user interface, select **Configuration | Appliances** and click **License**.

   Settings for importing a license appear on the settings pane.
2. Under **Import License**, click **end user license agreement** and review the agreement. Then select the checkbox in the same line.

   The **License File** field and the **Browse** button become available.
3. Click **Browse** and browse to the location where your license file is stored. Select the file and click **Activate**.

   The license is imported and license information appears below the input field.

An automatic update of important information for the appliance modules, for example, virus signatures, is started after the initial configuration. It can take several minutes and might not be completed after you have imported a license.

During this update, you cannot use the proxy functions of the appliance to access the web from the user interface.

Attempts to do so will lead to an error message stating that a module, for example, the Anti-Malware engine, cannot be loaded (because updated information is needed for this).

Port assignments

After setting up a hardware-based appliance, the ports of the appliance are assigned to the network interfaces on the hardware platform.

Each appliance model uses a particular server system as its hardware platform.

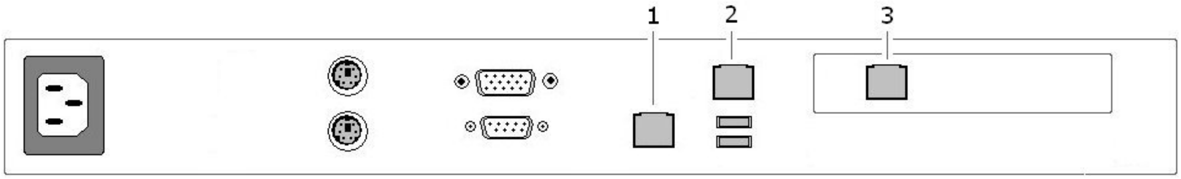
There are the following models:

- 4000B
- 4500B
- 5000B
- 5500B

The model number is located on a label on top of the hardware chassis. The diagrams in the following sections show the assignments of the network ports for each model.

4000B

This appliance model has three network interfaces on its rear panel.



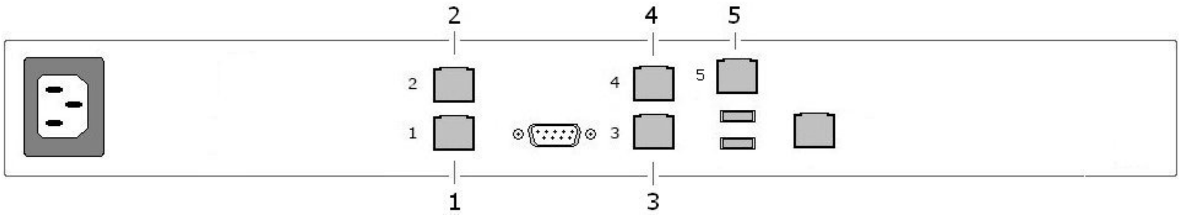
Ports assigned to these interfaces:

Position	Network interface	Port
1	e1000e	eth0
2	e1000	eth1
3	e1000e	eth2

On the *front panel* of this appliance model, the LED for network interface 2 lights up when you actually plug in network interface 1. Also when you plug in network interface 2, the LED for network interface 1 lights up.

4500B

This appliance model has five network interfaces on its rear panel.

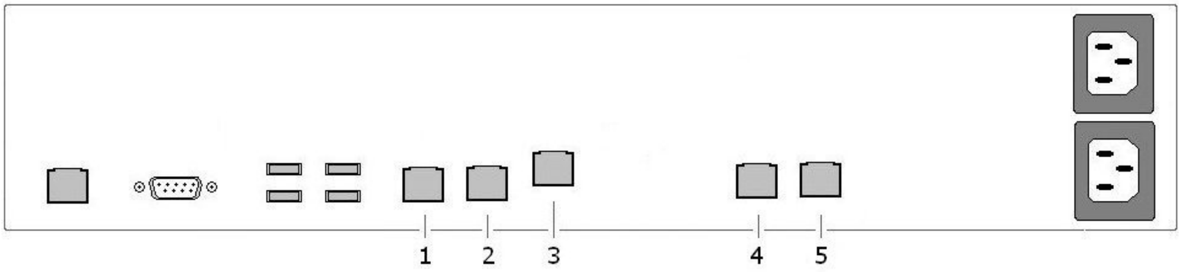


Ports assigned to these interfaces:

Position	Network interface	Port
1	igb	eth0
2	igb	eth1
3	igb	eth2
4	igb	eth3
5	e1000e	eth4

5000B

This appliance model has five network interfaces on its rear panel.

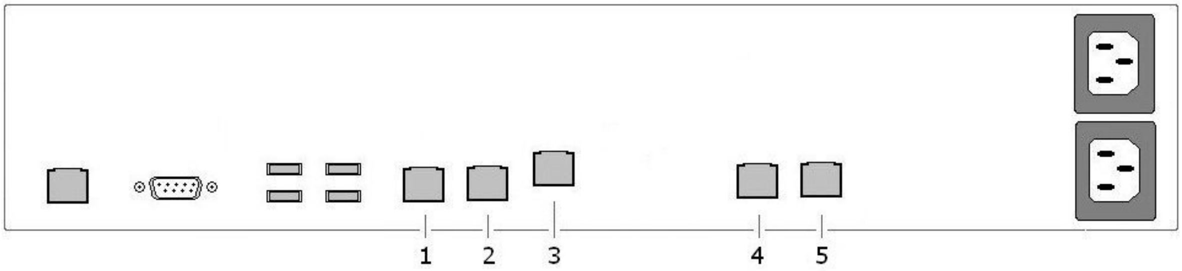


Ports assigned to these interfaces:

Position	Network interface	Port
1	igb	eth0
2	igb	eth1
3	rmm and bnc For operation of the RMM (Remote Management Module) controller	
4	e1000e	eth3
5	e1000e	eth2

5500B

This appliance model has five network interfaces on its rear panel.

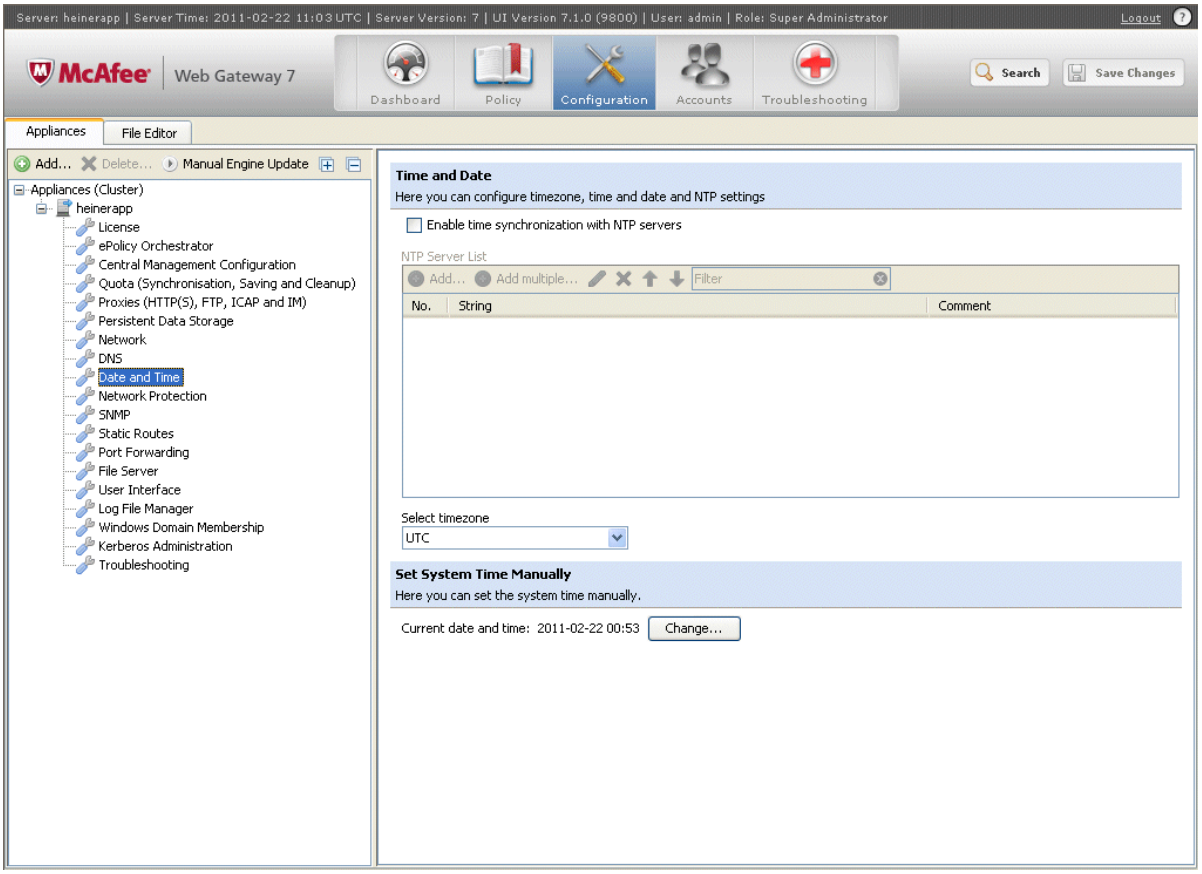


Ports assigned to these interfaces:

Position	Network interface	Port
1	igb	eth0
2	igb	eth1
3	rmm and bnc For operation of the RMM and BMC (Baseboard Management Controller) controllers	
4	e1000e	eth3
5	e1000e	eth2

User interface

The user interface allows you to work with rules, lists, settings, accounts, and other features of the appliance and to view information on key system parameters.



Server: heinerapp | Server Time: 2011-02-22 11:03 UTC | Server Version: 7 | UI Version 7.1.0 (9800) | User: admin | Role: Super Administrator

Time and Date

Here you can configure timezone, time and date and NTP settings

□ Enable time synchronization with NTP servers

NTP Server List

No.	String	Comment

Select timezone: UTC

Set System Time Manually

Here you can set the system time manually.

Current date and time: 2011-02-22 00:53 Change…

Main elements of the user interface

The following table describes the main elements of the user interface.

Table 2-4 Main elements of the user interface

Option	Definition
System information line	Displays system and user information.
Top-level menu bar	Lets you select one of the following menus: • **Dashboard** — For viewing information on events, web usage, filtering activities, and system behavior • **Policy** — For configuring your web security policy • **Configuration** — For configuring the system settings of the appliance • **Accounts** — For managing administrator accounts • **Troubleshooting** — For solving problems on the appliance
Tab bar	Provides the tabs of the currently selected top-level menu. The top-level menus have the following tabs: • **Dashboard** • Alerts • Charts and Tables • **Policy** • Rule Sets • Lists • Settings • **Configuration** • Appliances • File Editor • **Accounts** • Administrator Accounts The **Troubleshooting** top-level menu has no tabs.
Toolbar (on tab)	Provides varying tools (depending on the selected tab).
Navigation pane	Provides tree structures of configuration items, such as rules, lists, and settings.
Settings pane	Provides the settings of the item currently selected on the navigation pane for editing.
Logout	Logs you off from the user interface.
Help icon	Opens the online Help. You can browse through its pages or navigate on a tree structure and perform a full text search or search for index terms.
Search	Opens the **Search** window with the following options: • **Search for objects** — Lets you search for rule sets, rules, lists, and settings. Typing a search term in the input field displays all objects with names matching the search term. • **Search for objects referring to** — Lets you select a list, property, or settings and displays all rules that use the selected item.
Save Changes	Saves your changes.

Special configuration functions

The user interface provides several special functions to support your configuration activities.

Table 2-5 Special configuration functions

Option	Definition
Yellow triangle	Appears attached to the name of a list that is still empty and needs to be filled by you. Some filter lists are created, but not filled by the policy configuration wizard because they are too sensitive.
Yellow text insert	Appears when you move your mouse pointer over an item on the user interface providing information on the meaning and usage of the item.
OK icon	Appears in a window when the input you entered is valid.
False icon	Appears in a window when the input you entered is invalid.
Message text	Appears with the False icon, providing information on your invalid input.
Light red color of input field	Indicates an invalid entry.
Save Changes	The button turns red when you change an item. It turns gray again when you have saved your changes.
Red triangle	Appears attached to tabs, icons, and list entries when you have changed an item and not yet saved. For example, when you have changed a rule, the red triangle appears: • In the row of the rule entry on the settings pane • On the rule set icon • On the projection of the **Rule Sets** tab • On the **Policy** icon of the top-level menu bar

Discarding changes

When you have been performing administrator activities on the user interface, you can discard changes you have made instead of saving them.

One option to discard changes is a positive answer when prompted at logoff whether you really want to do it with unsaved changes.

Another option is to discard changes and reload configuration data.

Reloading configuration data restores the configuration that existed after it was last saved, which can have been done by you or another administrator. If no changes have been saved yet after the initial setup of the appliance, the initial setup configuration is restored.

Discard changes by reloading data

You can discard changes you have configured on the user interface by reloading the existing configuration data.

Task

1 Click the small black triangle next to the **Save Changes** button.

An insert reading **Reload Data from Backend** appears.

2 Click the insert.

Pending changes are discarded and the configuration data is reloaded.

3 Blade server

You can use a McAfee Blade as the hardware platform for McAfee Web Gateway.

Contents

McAfee Blade and blade system enclosure models

A McAfee Blade is the type of modular server commonly known as blade server. McAfee Blades are installed in blade system enclosures.

McAfee Web Gateway can run on the following two McAfee Blade models:

- ProLiant BL460c G6
- ProLiant BL460c G6.5

The following two enclosure models can be used for running McAfee Web Gateway:

- M3 (c3000)
- M7 (c7000)

Installation of the blade server system

To run McAfee Web Gateway on a McAfee Blade, you need to install the blade system enclosure with the blade servers.

A detailed description of this installation is provided in the documentation of the McAfee partner (Hewlett-Packard), which is available on their web site.

Installation requirements

You need to make sure the requirements for installing the blade server system are met.

For more information, see the *Site Planning Guide* and the *Setup and Installation Guide* for each enclosure model on the web site of the McAfee partner and the following sections.

Environment of the blade server system

You need to consider the environment you want to run the blade server system in.

- Power and air conditioning
- Integration of the blade servers into your network

Completeness of shipment

You need to go through the shipping list and check whether you have received the appropriate items.

- Blade system enclosure (M3 or M7) with McAfee Blades
- Power cords
- Network cables

IP addresses for the blade server system

The blade server system requires IP addresses for the following components:

- Onboard Administrator
- Integrated Lights Out (iLO) modules (between 8 and 16 addresses, depending on your configuration)
- Interconnect modules (four addresses)
- McAfee Blades (number of addresses depends on your configuration)

Install the blade server system

To install the blade server system, complete the following high-level steps.

Task

1. Make sure the requirements for the installation of the blade server system are met.
2. Set up the Onboard Administrator on the enclosure.
3. Set up Integrated Lights-Out Management.
4. Install the blade system enclosure.
5. Install the interconnect modules on the enclosure.
6. Supply power to the enclosure.

For more information, see the *Setup and Installation Guide* for each enclosure model, the *Onboard Administrator User Guide*, and the *Integrated Lights-Out User Guide* on the web site of the McAfee partner, as well as the following tasks.

Tasks

- *Install the blade system enclosure* on page 39
  To install the blade system enclosure:
- *Install the interconnect modules* on page 39
  The interconnect modules are installed in the interconnect bays on the blade system enclosure. These modules are either pass-through modules or switches.
- *Turn on the blade system enclosure* on page 39
  After installing the interconnect modules, you can supply power to the blade system enclosure and turn it on.

Install the blade system enclosure

To install the blade system enclosure:

Task

1. Review and observe the safety information that is provided.
2. Remove the protective packaging and place the blade system enclosure on a flat surface.

   Considering its weight, unpack the enclosure as close as possible to the intended location.

3. Remove the front and rear components, as well as the rear cage from the enclosure.
4. Install the power supplies, cooling fans, Interconnect modules and the Onboard Administrator.

   To ensure redundancy in the case of a power supply or cooling fan failure, we recommend that you install all available power supplies and fans.

5. Connect a monitor and keyboard to the enclosure.
6. Attach power cords to the monitor and the enclosure, but do not yet connect the power supplies of the enclosure.

Install the interconnect modules

The interconnect modules are installed in the interconnect bays on the blade system enclosure. These modules are either pass-through modules or switches.

The interconnect modules are installed in the interconnect bays on the blade system enclosure. These modules are either pass-through modules or switches.

The Onboard Administrator provides diagrams of the enclosure. Using the mouse-over function, you can locate the position of the interconnect bays on the rear side of the enclosure. The M3 enclosure model has four interconnect bays, the M7 model has eight.

Task

1. Locate the positions of the interconnect bays.
2. Install the interconnect modules as follows.
   - If your enclosure model is M3, install four switches in interconnect bays 1 to 4.
   - If your enclosure model is M7, install four switches in interconnect bays 1 to 4 and two pass-through modules in interconnect bays 5 and 6.

Turn on the blade system enclosure

After installing the interconnect modules, you can supply power to the blade system enclosure and turn it on.

Task

1. Connect the power cords of the enclosure to the power supplies and the power outlets.

   To ensure all blade servers on the enclosure turn on, use two power circuits.

   If you use only one circuit and the power management settings are configured for AC redundant (which is recommended) some blade servers will fail to turn on.

2. Turn on the blade system enclosure.

You can now install McAfee Web Gateway on a McAfee Blade in the enclosure.

Installation of McAfee Web Gateway on a McAfee Blade

To install McAfee Web Gateway on a McAfee Blade, you download the software, select a device for installation, and complete the installation procedure.

Software and installation devices

You can download the McAfee Web Gateway software in ISO or USB format from the Extranet for McAfee Web Gateway.

You can use different devices to install McAfee Web Gateway on a McAfee Blade, depending on your enclosure model:

- Internal CD/DVD-ROM drive (M3)
- External CD/DVD-ROM drive (M7)
- USB drive (M3 and M7)
- Virtual media (M3 and M7)

Install McAfee Web Gateway using the internal CD/DVD-ROM drive

If your enclosure model is M3, you can use the internal CD/DVD-ROM drive to install McAfee Web Gateway.

Task

1. Insert a CD or DVD with the McAfee Web Gateway software on it into the internal CD/DVD-ROM drive on the enclosure.
2. Open the Onboard Administrator of the enclosure and select the McAfee Blade you want to install McAfee Web Gateway on.
3. Click the **Virtual Devices** tab.
4. Use this tab to connect the internal CD/DVD-ROM drive to the blade server.
5. Click the **Boot Options** tab and set **One Time Boot from** to `CD-ROM`.
6. Turn on the blade server.

   The installation menu for McAfee Web Gateway appears.

You can now select an installation mode from the menu and install McAfee Web Gateway.

See also
Install the appliance software using the installation menu on page 22

Install McAfee Web Gateway using an external CD/DVD-ROM drive

If your enclosure model is M7, you can use an external CD/DVD-ROM drive to install McAfee Web Gateway.

Task

1 Insert a CD or DVD with the McAfee Web Gateway software on it into the external CD/DVD-ROM drive.

2 Use the USB SUV cable that is shipped with the enclosure to connect the external CD/DVD-ROM drive to the McAfee blade you want to install McAfee Web Gateway on.

3 Open the Onboard Administrator of the enclosure and select the appropriate McAfee Blade.

4 Click the **Boot Options** tab and set **One Time Boot from** to `CD-ROM`.

5 Turn on the blade server.

The installation menu for McAfee Web Gateway appears.

You can now select an installation mode from the menu and install McAfee Web Gateway.

See also

Install the appliance software using the installation menu on page 22

Install McAfee Web Gateway using a USB drive

You can use a USB drive to install McAfee Web Gateway on one of the servers in the blade system enclosure.

Task

1 Use the USB SUV cable that is shipped with the enclosure to connect the USB drive to the McAfee Blade you want to install McAfee Web Gateway on.

2 Open the Onboard Administrator of the enclosure and select the appropriate McAfee Blade.

3 Click the **Virtual Devices** tab.

4 Click the **Boot Options** tab and set **One Time Boot from** to `USB`.

5 Turn on the blade server.

The installation menu for McAfee Web Gateway appears.

You can now select an installation mode from the menu and install McAfee Web Gateway.

See also

Install the appliance software using the installation menu on page 22

Install McAfee Web Gateway using virtual media

The blade system enclosure provides an option for a virtual installation of McAfee Web Gateway on a server in the enclosure using an ISO image that is stored on one of your local drives.

Task

1. Open the Onboard Administrator of the enclosure and select the McAfee Blade you want to install McAfee Web Gateway on.
2. Click **iLO**, then click **Web Administration**.

   A new browser window opens providing access to the iLO (integrated Lights-Out) web user interface.
3. Click the **Virtual Media** tab, then click *Virtual Media*.

   The Virtual Media window opens.
4. Choose the Virtual Floppy/USB Key or Virtual CD/DVD-ROM option for installing the ISO image and click **Browse** in the relevant section. Then browse to the ISO image file you want to install.
5. Click **Connect**.

   The ISO image is made available for installation and the installation menu for McAfee Web Gateway appears.

You can now select an installation mode from the menu and install McAfee Web Gateway.

See also
Install the appliance software using the installation menu on page 22

Network setup

After installing McAfee Web Gateway on a McAfee Blade, you can configure the network setup.

You can configure one of the following setups:

- Proxy HA (High Availability)
- Proxy with external load balancing
- Transparent router
- Transparent bridge

For each of these setups, you need to configure the appropriate settings on the user interface of McAfee Web Gateway and complete additional configuration activities for the other network components.

See also
Proxies settings on page 118

Proxy HA (High Availability)

You can configure McAfee Web Gateway on a McAfee Blade to provide the functions of a proxy that runs in explicit proxy mode and is a part of a High Availability configuration.

Network configuration

We recommend that you configure the proxy HA network setup as a two-legged proxy solution. This means that two separate interfaces are used for inbound and outbound web traffic.

As this is a High Availability configuration, there must be at least two director nodes, so a fail-over can be performed in case on them is down. A director node ensure load balancing is performed by directing data packets in a suitable manner to the nodes that only scan the data. It is configured with a director priority higher than zero whereas this parameter is set to zero for scanning nodes.

On a director node, you need a virtual IP address for the interface that handles the inbound web traffic. This address is assigned according to the VRRP (Virtual Router Redundancy Protocol).

We also recommend to use the outbound network interface on a director node for load-balancing the web traffic. To achieve this, you need to specify the IP address that the outbund network interface has as a physical component when configuring the management IP address as part of the proxy settings.

You should furthermore use an additional interface for out-of-band management, which allows you to perform management communication separately.

Link resilience

If the interconnect modules you are using are switches, we recommend that you bundle two of the uplink ports on the switches to a trunk group.

This way you can achieve link resilience since you can connect each uplink port by a network cable to provide it with a physical link. If one of the two links fails, the trunk group remains still active.

For the VRRP interface, no uplink ports are required because this interface is only used for internal communication within the Blade system enclosure.

The following table shows an example of how you can assign trunk groups, interconnect modules, and interfaces to each other in a proxy HA network setup.

Table 3-1 Assignment of network components in a proxy HA network setup

Network interface port	Interconnect module	Trunk group
Inbound web traffic interface	Switch in interconnect bay 1	Group 1: port 21, port 22
Outbound web traffic interface	Switch in interconnect bay 2	Group 2: port 21, port 22
Out-of-band management interface	Switch in interconnect bay 3	Group 3: port 21, port 22
VRRP interface	Switch in interconnect bay 4	no uplink ports required

For more information on how to configure the interconnect modules, see the *GbE2c Ethernet Blade Switch for c-Class BladeSystem Application Guide* on the web site of the McAfee partner.

Proxy with external load balancing

You can configure McAfee Web Gateway on a McAfee Blade to provide the functions of a proxy that runs in explicit proxy mode and have availability ensured by using an external load balancer.

Network configuration

We recommend that you configure the explicit proxy with load balancing setup as a two-legged proxy solution. This means that two separate interfaces with an IP address for each of them are used for inbound and outbound web traffic.

You should use an additional interface for out-of-band management, which allows you to perform management communication separately.

Link resilience

If the interconnect modules you are using are switches, we recommend that you bundle two of the uplink ports on the switches to a trunk group.

This way you can achieve link resilience since you can connect each uplink port by a network cable to provide it with a physical link. If one of the two links fails, the trunk group remains still active.

The following table shows an example of how you can assign trunk groups, interconnect modules, and interfaces to each other in an explicit proxy with load balancing setup.

Table 3-2 Assignment of network components in in an explicit proxy with load balancing setup

Network interface port	Interconnect module	Trunk group
Inbound web traffic interface	Switch in interconnect bay 1	Group 1: port 21, port 22
Outbound web traffic interface	Switch in interconnect bay 2	Group 2: port 21, port 22
Out-of-band management interface	Switch in interconnect bay 3	Group 3: port 21, port 22

For more information on how to configure the interconnect modules, see the *GbE2c Ethernet Blade Switch for c-Class BladeSystem Application Guide* on the web site of the McAfee partner.

Load balancer

Load balancing is performed in this configuration by an external device that assigns load to individual blade servers. For this purposes, the blade servers are included in a load balancing pool.

When you configure the load balancer, you should use an algorithm that supports IP client stickiness. This ensures that functions requiring IP client stickiness, such as the progress page, are available.

Transparent router

You can configure McAfee Web Gateway on a McAfee Blade to provide the functions of a transparent router that directs web traffic between different segments of your network.

We recommend that you configure the transparent router network setup as a two-legged proxy solution. This means that two separate interfaces with a virtual IP address for each of them are used for inbound and outbound web traffic.

The virtual IP addresses are assigned according to the VRRP (Virtual Router Redundancy Protocol).

We also recommend to use the outbound network interface for load-balancing the web traffic. To achieve this, you need to specify the IP address that the outbund network interface has as a physical component when configuring the management IP address as part of the proxy settings.

If IP spoofing is enabled, the nodes that are only used for scanning within this setup, do not need a connection for inbound web traffic. Inbound and outbound traffic are all handled by the director node that does the load-balancing,

Transparent bridge

You can configure McAfee Web Gateway on a McAfee Blade to provide the functions of a transparent bridge between different segments of your network.

We recommend that you configure the transparent bridge network setup as a two-legged proxy solution. For the network mode, the two-legged solution does not require virtual IP addresses and no communication under VRRP is performed accordingly.

The director node that does the load-balancing is assigned this role according to the STP (Spanning Tree Protocol).

When configuring the management IP address as part of the proxy settings, you need to specify the IP address of the *ibr0* bridge interface.

To ensure the director node is correctly assigned under STP, you need to disable the use of STP on the blade switches for inbound and outbound web traffic. STP is then executed by the operating system.

Port identification

When McAfee Web Gateway is running on a McAfee Blade, it uses the network interfaces of this blade server. Assignment of ports, such as eth0, eth1, and so on, to these network interfaces varies with different McAfee Blade models.

The network interfaces are located on the system board of a server and on additional network interface cards (Mezzanine cards).

The ports that are assigned to the network interfaces are physically provided by interconnect modules, which can be:

- Pass-through modules (HP 1Gb Ethernet Pass-Thru Modules)
- Switches (HP GbE2c Layer 2/3 Ethernet Blade Switches, also known as LAN interconnects)

These modules are installed in the interconnect bays of the blade system enclosure. Each network interface has a port provided and mapped to an interconnect bay.

Ports provided by pass-through modules and switches

A pass-through module on a blade system enclosure provides 16 ports. This means a port can be assigned to a network interface for each of the 16 blade servers that can be contained in an enclosure.

However, a switch provides only five uplink ports. It is then a matter of configuration which servers have ports provided for their network interfaces, so that a port assignment can be made for them.

The mapping of ports for network interfaces to pass-through modules and switches can be viewed using the Onboard Administrator of the enclosure in question.

Mapping of ports for network interfaces

Ports for network interfaces on blade servers are mapped to the interconnect bays of the blade system enclosure.

The mapping is the same for all servers. For example, the port for the first network interface on the system board of a server is always mapped to interconnect bay 1.

There can be up to eight network interfaces on a Blade server:

- 2 LoM (LAN on motherboard) network interfaces embedded on the system board
- 2 network interfaces on Mezzanine card 1
- 4 network interfaces on Mezzanine card 2

The M3 enclosure model provides four interconnect bays, the M7 model provides eight. On the former model, two network interface ports are always mapped to one interconnect bay.

However, some of the interconnect bays can be empty, which means they cannot be included in the mapping then.

The following tables show the mapping for each enclosure model with all interconnect bays occupied.

Table 3-3 Port mapping on M3 enclosure

Network interface port	Interconnect bay
LoM 1 port	1
LoM 2 port	1
Mezzanine card 1 – port 1	2
Mezzanine card 1 – port 2	2
Mezzanine card 2 – port 1	3
Mezzanine card 2 – port 2	4
Mezzanine card 2 – port 3	3
Mezzanine card 2 – port 4	4

Table 3-4 Port mapping on M7 enclosure

Network interface port	Interconnect bay
LoM 1 port	1
LoM 2 port	2
Mezzanine card 1 – port 1	3
Mezzanine card 1 – port 2	4
Mezzanine card 2 – port 1	5
Mezzanine card 2 – port 2	6
Mezzanine card 2 – port 3	7
Mezzanine card 2 – port 4	8

Assignment of ports to network interfaces

Assignment of ports, such as eth0, eth1, and so on, to network interfaces on blade servers varies depending on the server model.

The assignment depends also on the type of network interface card that provides the port.

The following tables show the port assignments for each server model and network interface card.

Table 3-5 Port assignments on G6 server model

Network interface port	Port assignment	Network interface card
LoM 1 port	eth6	HP NC 352i
LoM 2 port	eth7	
Mezzanine card 1 – port 1	eth0	HP NC 360m
Mezzanine card 1 – port 2	eth1	
Mezzanine card 2 – port 1	eth2	HP NC 364m
Mezzanine card 2 – port 2	eth3	
Mezzanine card 2 – port 3	eth4	
Mezzanine card 2 – port 4	eth5	

Table 3-6 Port assignments on G6.5 server model

Network interface port	Port assignment	Network interface card
LoM 1 port	eth6	HP NC 352i
LoM 2 port	eth7	

Table 3-6 Port assignments on G6.5 server model *(continued)*

Network interface port	Port assignment	Network interface card
Mezzanine card 1 – port 1	eth4	HP NC 382m
Mezzanine card 1 – port 2	eth5	
Mezzanine card 2 – port 1	eth0	HP NC 364m
Mezzanine card 2 – port 2	eth1	
Mezzanine card 2 – port 3	eth2	
Mezzanine card 2 – port 4	eth3	

4 Rules

Web filtering and authentication is controlled by rules, which you can implement and modify to let them suit the needs of your network.

Rules are grouped and made available in rule sets, each of which usually covers a particular field of filtering activities. There can be, for example, a virus and malware filtering rule set, a URL filtering rule set, an authentication rule set, and so on.

At the initial setup of the appliance, you are asked to implement an initial system of rule sets, which can be the default system or a system that a wizard sets up according to your specifications.

You can then review the rules and rule sets of the implemented system, modify and delete them, and also create your own rules and ruie sets or even a complete system of your own.

In addition to the rule sets of the initial system, you can import rule sets from a library and modify them in the same way as the initial rule sets.

Contents

About filtering

A filtering process is performed on the appliance that uses the implemented rules to ensure web security for your network.

This process filters web traffic. It blocks some objects and lets others pass through, like a tea sieve or strainer that catches the tea leaves and allows the liquid to flow through its perforations.

How does the process tell the tea leaves from the liquid? The tea strainer obviously uses size as a key concept. If something is too big, it cannot pass through.

Similarly, the filtering process on the appliance uses in its rules all kinds of properties that web objects can have or that are related in some way to web objects to make filtering decisions.

Properties of filtered objects

A property of a web object checked in the filtering process is, for example, *being virus-infected*. A web object can have the property of being virus-infected, put more simply, it can be virus-infected.

Other examples could be the property of belonging into a particular URL category or the property of having a particular IP address.

The following can then be asked about these and other properties:

- *For a given web object, what value does property p have?*
- *And: If this value is x, what action is required?*

Giving an answer to the second question leads to a rule:

If the value of property p is x, action y is required.

A property is a key element in every rule on the appliance. Understanding the property is essential to understanding the rule.

When you are creating a rule, it is a good idea to begin by thinking about the property you want to use. Using a property of an already existing rule as an example, you might consider something like the following:

I want to filter viruses and other malware. I use the property of being virus-infected and build a rule around it. I let this rule require a blocking action to be taken if a given web object has this property.

The rule could look as follows:

If being virus-infected has the value true (for a given web object), block access to this object.

The web object could, for example, be a file that a web server has sent because a user of your network requested it and that is intercepted and filtered on the appliance.

Properties and rules are explained in this section using normal language. However, the format they have on the user interface of the appliance does not differ from this very much.

For example, the above rule about virus infections could appear on the user interface as follows:

Antimalware.Infected equals true –> Block (Default)

where *Antimalware.infected* is the property and *Block* is the action, which is executed in the default way.

The arrow does not appear on the user interface, it is inserted here to show that the blocking action is triggered if a given web object really has the property in question.

Filtering users

Properties can be related to web objects, but also to the users that request them.

For example, a rule could use the property *user groups that user is member of* to block requests sent by users who are not in an allowed group:

If user groups that user is member of (for a given user) are not on the list of allowed groups, block requests sent by this user.

Filtering cycles

The filtering process on the appliance has three cycles: the request cycle, the response cycle, and the embedded objects cycle. Only one of them can go on at a given moment.

The request cycle is performed for filtering requests that users of your network send to the web, the response cycle is for the responses received upon these requests from the web.

When embedded objects are sent with requests or responses, the embedded objects cycle is performed as an additional cycle of processing.

An embedded object could, for example, be a file sent with a request to upload a file and embedded in this file. The filtering process begins with the request cycle, filtering the request and checking the file that is requested for uploading. Then the embedded objects cycle is started for the embedded file.

Similarly, the response cycle and the embedded objects cycle are started one after another for a file that is sent in response from a web server and has another file embedded in it.

For every rule on the appliance, it is specified in which cycle it is processed. However, the cycle is not specified individually for a rule, but for the rule set that contains it.

A rule set can be processed in just one cycle or in a combination of cycles.

Process flow

In the filtering process, the implemented rules are processed one after another, according to the positions they take in their rule sets.

The rule sets themselves are processed in the order of the rule set system, which is shown on the **Rule Sets** tab of the user interface.

In each of the three cycles, the implemented rule sets are looked up one after another to see which must be processed in this cycle.

When a rule is processed and found to apply, it triggers an action. The action executes a filtering measure, such as blocking a request to access a web object or removing a requested object.

In addition to this, an action has an impact on the filtering process. It can specify that the filtering process must stop completely, or skip some rules and then continue, or simply continue with the next rule.

Processing also stops after all implemented rules have been processed.

Accordingly, the process flow can be as follows:

All rules have been processed for each of the configured cycles and no rule has been found to apply. –> Processing stops.

In the request cycle, the request is allowed to pass through to the appropriate web server.

In the response cycle, the response sent from the web is forwarded to the appropriate user.

In the embedded objects cycle, the embedded object is allowed to pass through with the request or response it was sent with.

Processing begins again when the next request is received.

A rule applies and requires that processing must stop completely. –> Processing stops.

An example of a rule that stops processing completely is a rule with a blocking action.

If, for example, a request is blocked because the requested URL is on a blocking list, it is no use to process anything else.

No response is going to be received because the request was blocked and not passed on to the appropriate web server. Filtering an embedded object that might have been sent with the request is also not needed because the request is blocked anyway.

A message is sent to the user who is affected by the action, for example, to inform this user that the request was blocked and why.

Processing begins again when the next request is received.

A rule applies and requires that processing must stop for the current rule set. –> Processing stops for this rule set.

The rules that follow the stopping rule in the rule set are skipped.

An example of a rule that stops the processing of a rule set is a whitelisting rule followed by a blocking rule in the same rule set.

When a requested web object is found on a whitelist, the request is allowed to pass through without further filtering. Therefore the rule set is not processed any further and the rule that eventually blocks the object is skipped.

Processing continues with the next rule set.

The next rule set can contain rules that, for example, block a request, although it was allowed to pass through the preceding rule set.

A rule applies and requires that processing must stop for the current cycle. –> Processing stops for this cycle.

The rules and rule sets that follow the stopping rule in the cycle are skipped.

An example of a rule that stops the processing of a cycle is a global whitelisting rule.

When a requested object is found on a global whitelist, the request is allowed to pass through to the appropriate web server. To ensure the request is not blocked eventually by any of the following rules and rule sets, the request cycle is not processed any further.

Processing continues with the next cycle.

A rule applies and requires that processing continues with the next rule. –> Processing continues with the next rule.

This can be the next rule in the current rule set or the first rule in the next rule set or cycle.

An example of a rule that lets the filtering process continue unimpeded is a statistics rule.

This rule just counts requests by increasing a counter and does otherwise nothing.

Rule elements

A web security rule on the appliance has three main elements: *criteria*, *action*, and (optionally) *event*.

1 **Criteria**

Determines whether a rule applies.

> Other rule syntaxes use the term *condition* instead of *criteria*.

If the category of a URL is on list x, ...

The criteria has three elements: *property*, *operator*, and *operand*

- **Property**

  Is related to a web object or a user.

  … the category of a URL …

- **Operator**

  Links the property to an operand.

  … is on list …

- **Operand**

  Specifies a value that the property can have.

  … x (list name), …

  The operand is also referred to as *parameter* on the user interface.

2 **Action**

Is executed if the criteria is matched.

… block the URL …

3 **Event**

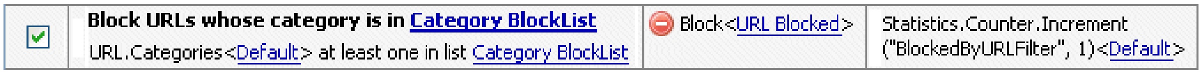
Is executed if the criteria is matched.

… and log this action.

An event is optional for a rule. A rule can also have more than one event.

Rule format on the user interface

On the user interface, a rule appears in the following format.



☑	**Block URLs whose category is in Category BlockList** URL.Categories<Default> at least one in list Category BlockList	Block<URL Blocked>	Statistics.Counter.Increment ("BlockedByURLFilter", 1)<Default>

Figure 4-1 Format of a rule on the user interface

The following table explains the meaning of the rule elements.

Table 4-1 Elements of a rule on the user interface

Option	Definition
Enabled	Allows you to enable or disable the rule.
Name	Name of the rule • **Block URLs …** — Name text • **Category BlockList** (in rule name) — List used by the rule Clicking on the list name opens the list for editing. • Yellow triangle (next to a list name) — Indicates that the list is initially empty and you need to fill the entries.

Table 4-1 Elements of a rule on the user interface *(continued)*

Option	Definition
Criteria	Criteria of the rule The criteria is only visible after clicking the **Show details** toggle button. • **URL.Categories** — Property • **<Default>** — Settings of the module that retrieves a value for the property For example, the *Default* settings that appear here are settings of the URL Filter module. Clicking on the settings name opens the settings for editing. The module name is not visible in the rule. It appears, however, in the **Edit** window for the rule criteria. • **at least one in list** — Operator • **Category BlockList** — Operand (also known as parameter) Clicking on the list name opens the list for editing. The list name appears both in the rule name and the criteria to let it be available when the criteria is not visible. • Yellow triangle (next to a list name) — Indicates that the list is initially empty.
Action	Action of the rule • **Block** — Name of the action • **<URLBlocked>** — Settings of the action Clicking on the settings name opens the settings for editing.
Events	One or more events of the rule The events are only visible in full after clicking the **Show Details** toggle button. • **Statistics.Counter. Increment** — Name of the event • **“BlockedByURLFilter, 1”** — Parameters of the event • **<Default>** — Settings of the event Clicking on the settings name opens the settings for editing.

Complex criteria

The criteria of a rule can be made complex by configuring it with two or more parts.

In complex criteria each of the parts has a property with operator and operand. The parts are linked by AND or OR.

The criteria is matched if a filtered URL belongs to a category that is on any of the two specified category lists (or on both).

If you configure criteria with three or more parts and use both AND and OR between them, you also need to put brackets to indicate how the parts are logically connected. For example, (a AND b) OR c differs in meaning from a AND (b OR c).

When you add a third criteria part on the user interface, lowercase letters appear before the parts and an additional field is inserted at the bottom of the configuration window.

The field displays your criteria parts in short, for example, a AND b OR c. You can then type brackets in the field as needed.

Rule sets

Rules are grouped and included in rule sets on the appliance. A rule can never stand on its own, it must be included in a rule set.

A rule set can include just a single rule or several of them. It can also include one or more nested rule sets. If it includes nested rule sets, it can include individual rules on the same level as the nested rule sets.

Rule sets usually include rules that work together to provide a particular function for ensuring web security.

For example, a virus and malware filtering rule set will include a rule that blocks infected rule sets and one or several others that whitelist objects to let them skip the blocking rule and ensure users can access them.

You can modify the implemented rule sets and create rule sets of your own to build functional units in whatever way is suitable for your network.

Rule set criteria

Like rules, rule sets have criteria and are applied if their criteria matches.

Usually, the criteria of a rule set differs from that of its rules. For a rule to apply, both its own criteria and the criteria of its rule set must match.

Rule set cycles

Rule sets are processed, with their rules, in the three cycles of the filtering process.

A rule set can be processed in any combinations of these cycles, for example, only in the request cycle or in both request and response cycles, and also in all three cycles.

The cycles of a rule set are at the same time those of the individual rules it includes. A rule cannot differ with regard to cycles from its rule set.

Nested rule sets

Rule sets can have other rule sets nested within them. A nested rule set has its own criteria.

Regarding cycles, it can only be processed in the cycles of the nesting rule set, but need not be processed in all of them.

This way, a nested rule set can be configured to deal especially with a particular cycle, while another nested rule set deals with a different cycle.

For example, a media type filtering rule set could apply to all cycles, but have nested rule sets that are not processed in all of them.

Media Type Filtering rule set (for requests, responses, and embedded objects)

- Nested rule set *Media Type Upload*(for requests)
- Nested rule set *Media Type Download* for responses and embedded objects)

Rule set system

Rule sets are implemented on the appliance as part of a rule set system.

After a request for web access sent by a user of your network has been received on the appliance, all rule sets in the system are processed from top to bottom.

When a rule in a rule set is found to apply, the action of this rule is executed. If the action is Block, processing stops. Other actions let processing continue in one or the other way.

Similarly, the rule sets of the implemented system are processed for responses and embedded objects.

Working with the rule set system

When working with the rule set system, you can do the following:

- **Implement an initial rule set system** — During the initial setup of the appliance
- **Modify the implemented rule set system** — After the initial setup to finetune the system and adapt it to the needs of your network

  When modifying the system, you can:

  - Modify rules and rule sets
  - Delete rules and rule sets
  - Create new rules and rule sets
  - Import rule sets
  - Move rules and rule sets to new positions
  - Copy rules and paste them into other rule sets

Initial rule set systems

During the initial setup of the appliance, you are asked to implement a initial rule set system.

You can implement the following:

- **Wizard-created rule set system** — A system that the Policy Creation Wizard creates according to your selections

  You can make selections regarding the type of your organization, regional location, and restrictiveness.

- **Default rule set system** — The default system

  This system is implemented if you make no selections.

After the initial setup, you can review and modify both types of systems in the same way.

Rule set library

The rule set library provides additional rule sets that you can import into the implemented rule set system.

The library also contains the rule sets of the default rule set system.

The URL Filtering and Media Type Filtering rule sets exist in the default system in three versions that allow filtering for different user groups.The library contains a standard version for each of the two rule sets.

Sample initial rule set systems

The following two tables show samples of initial rule set systems. One is a wizard-created rule set system, the other is the default rule set system. Nested rule sets are not shown.

The wizard-created ruie set system reflects the following selections: Type of organization — *commercial*, location — *Europe*, level of strictness — *limited (medium)*.

Table 4-2 Wizard-created rule set system

Rule set	Description
Global Whitelist	Lets requests for whitelisted URLs or IP addresses skip further filtering
Global Block	Blocks requests when the requested URLs or IP addresses are on block lists
Media Type Filtering	Controls media type filtering with nested rule sets for uploading and downloading media types
Content Filter	Exempts users if entered in a whitelist. Blocks users if entered in a blocking list. Blocks URLs belonging to various categories
Gateway AntiMalware	Controls virus and malware filtering using virus signatures and proactive methods
SSL Scanner	Prepares SSL-secured web traffic for processing by other filtering functions with nested rule sets for certificate verification and inspection enabling

The default rule system looks like this.

Table 4-3 Default rule set system

Rule set	Description
SSL Scanner *(not enabled by default)*	Prepares SSL-secured web traffic for processing by other filtering functions with nested rule sets for certificate verification and inspection enabling
Global Whitelist	Lets requests for whitelisted URLs or IP addresses skip further filtering
Common Rules	Provides functions that support the filtering process, such as web caching, progress indication, and opening of archives
Authenticate and Authorize *(not enabled by default)*	Asks unauthenticated users to authenticate and blocks users who are not in an allowed user group with nested rule sets for both functions
Content Filter for Unauthenticated User	Controls filtering of individual URLs, URL categories, and media types for unauthenticated users
Content Filter for User Group "internet"	Controls filtering of individual URLs, URL categories, and media types for users belonging to a particular user group
Content Filter for User Group "internet_strict"	Controls filtering of individual URLs, URL categories, and media types for users belonging to a user group that has a stricter blocking level applied to it This can be achieved, for example, by using block lists containing more or different entries compared to the lists used for the other groups.
Gateway AntiMalware	Controls virus and malware filtering using virus signatures and proactive methods

Rule set library

The rule set library provides rule sets for you to import into your rule set system.

You can import a rule set, for example, to to add a function that is missing in your system or when the implemented rule sets do not suit your network.

The rule set library contains also the rule sets that are part of the default rule set system.

More rule sets are available from an online rule set library. A link to this library is provided in the window of the standard rule set library.

The following table shows the rule sets of the standard rule set library (nested rule sets are not shown).

Table 4-4 Library rule sets

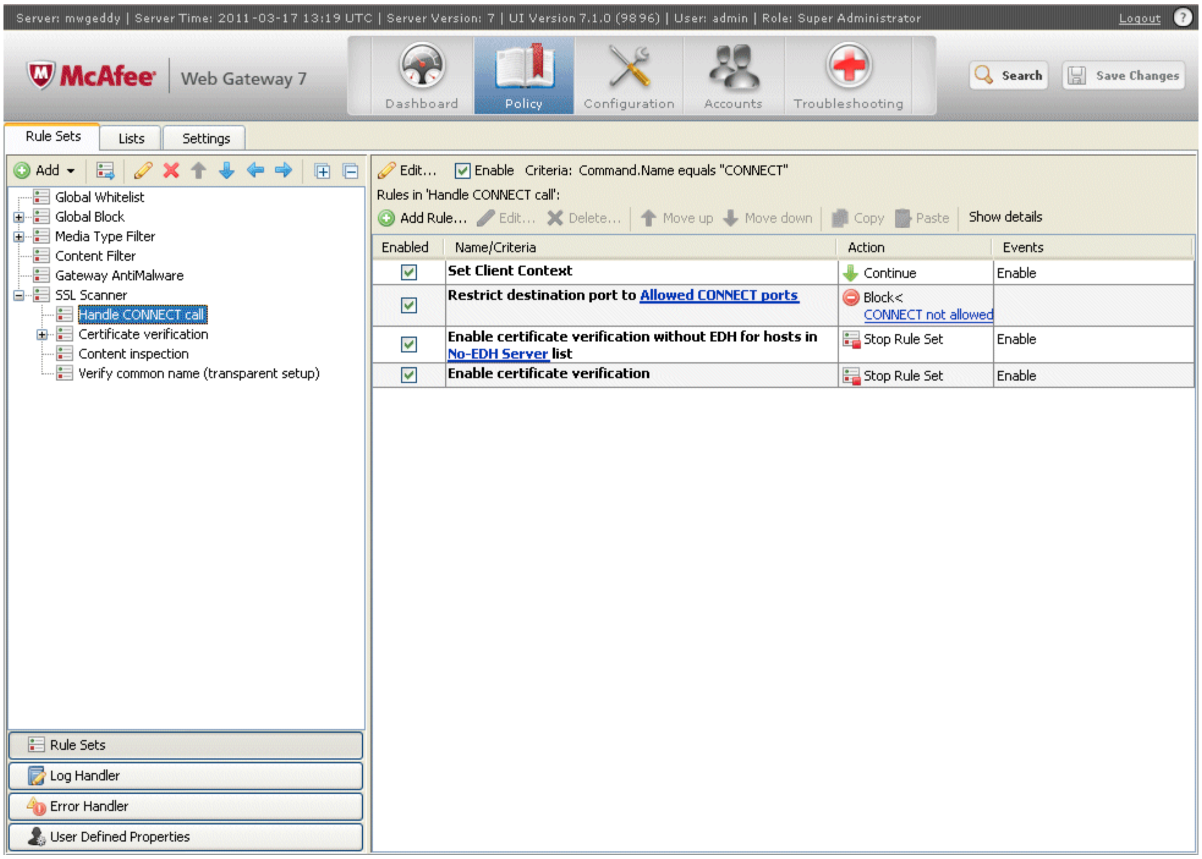
Rule set	Description
Access Log	Logs user requests for web access
Access Log With Cache Status	Logs user requests for web access and cache status
Authentication Server	Handles authentication on an authentication server
Authorized Override	Allows users to continue when the configured quota for web usage has been exceeded
Block on All Errors	Blocks requests when an internal error has occurred on the appliance
Block on Antimalware Engine Errors	Blocks requests when the Anti-Malware module cannot be loaded or is overloaded
Block on URL Filter Errors	Blocks requests when the URL Filter module cannot be loaded or is overloaded
Blocking Sessions	Blocks users for a period of time after trying to access to web objects that were not allowed.
Bypass ePO Requests	Lets connection requests sent from an ePO server skip filtering
Coaching	Ask users to confirm usage of web pages before they are allowed to continue
Common Rules	Provides functions that support the filtering process, such as web caching, progress indication, and opening of archives
Cookie Authentication	Controls authentication using cookies and retrieving information from an authentication server
Cookie Authentication with Login Page	Controls authentication using cookies and retrieving information from an authentication server when users provide their credentials on a logon page
Data Leakage Prevention	Controls traffic flow between the appliance and a DLP solution
Direct Proxy Authenticate and Authorize	Asks unauthenticated users to authenticate and blocks users who are not in an allowed user group with nested rule sets for both functions
Enable Opener	Enables the module that opens multi-part objects, for example, archives
Found Viruses Log	Logs the names of viruses found by the Anti-Malware module
Gateway Antimalware	Controls virus and malware filtering using virus signatures and proactive methods
Global Block	Blocks requests when the requested URLs or IP addresses are on block lists
Global Whitelist	Lets requests for whitelisted URLs or IP addresses skip further filtering
Handle Special Sites	Handles communication with special whitelisted web servers and provides solutions for some communication problems

Table 4-4 Library rule sets *(continued)*

Rule set	Description
Handle Update Incidents	Logs incidents concerning updates and sends various kinds of notifications
HTML Filtering	Filters HTML pages and uses its nested rule sets to remove embedded objects, such as Java scripts and others, from these pages
ICAP Client	Controls traffic flow between the appliance and an ICAP server
IM Authentication	Controls authentication for users who communicate with the appliance using aninstant messaging protocol
IM Logging	Records requests received on the appliance under an instant messaging protocol
Log File Manager Incidents	Logs incidents concerning the Log File Manager and sends various kinds of notifications
Long Running Connections	Enables you to keep long running connections alive
Lookup User Name from Proxy Authorization BasicHeader	Retrieves information for authenticating users by a lookup based on the proxy authorization header
Media Type Filtering	Controls media type filtering with nested rule sets for uploading and downloading media types
Monitoring	Checks CPU overload, cache partitions, and request overload
Next Hop Proxy	Ensures that internal hosts are used as next-hop proxy servers for internal requests
Progress Indication	Enables display of progress page and data trickling as means of indicating download progress to the user
Remove Header	Removes “via” information from the a request header
Script Filter	Filters web pages for embedded script code and removes it
SiteAdvisor Enterprise Interlock	Blocks request to force SiteAdvisor Enterprise into stand-down mode
SSL Scanner	Prepares SSL-secured web traffic for processing by other filtering functions with nested rule sets for certificate verification and inspection enabling
Time Quota	Allows users web usage only for a configured period of time per day, week, or other time units
Try-Auth	Asks unauthenticated users to authenticate and blocks users who are not in an allowed user group with nested rule sets for both functions
URL Filtering	Controls filtering of individual URLs and URL categories
Volume Quota	Allows users web usage only as long as a configured amount of bytes per day, week,or other time units is not exceeded
Web Cache	Controls caching of web objects with nested rule sets for reading from and writing to the cache
Welcome Page	Controls display of a welcome page to users

Rule Sets tab

The **Rule Sets** tab allows you to work with rules and rule sets.



☑ Enable Criteria: Command.Name equals "CONNECT"

Rules in 'Handle CONNECT call':

Enabled	Name/Criteria	Action	Events
☑	Set Client Context	Continue	Enable
☑	Restrict destination port to Allowed CONNECT ports	Block< CONNECT not allowed	
☑	Enable certificate verification without EDH for hosts in No-EDH Server list	Stop Rule Set	Enable
☑	Enable certificate verification	Stop Rule Set	Enable

Main elements of the Rule Sets tab

The following table describes the main elements of the **Rule Sets** tab.

Table 4-5 Main elements of the Rule Sets tab

Element	Description
Rule sets toolbar	Items for working with the rule sets on the rule sets tree
Rule sets tree	Tree structure displaying the rule sets of the appliance configuration
Rule sets menu	Buttons for displaying tree structures of: • (General) rule sets • Log handler rule sets • Error handler rule sets • User-defined properties (for use in rule set criteria, rule criteria, and rule events)
Rules toolbar	Items for working with rules
Rules	Rules of the currently selected rule set

Rule sets toolbar

The rule sets toolbar provides the following options.

Table 4-6 Rule sets toolbar

Option	Definition
Add	Opens a menu or a window for adding an item, depending on what is currently selected from the Rule sets menu. • (**Rule Sets** is selected) — Opens a menu, from which you can select: • **Rule Set from Library** — Opens the **Add from Rule Set Library** window for importing a rule set from the rule set library. • **Rule Set** — Opens the **Add New Rule Set** window to let you add a rule set to the appliance configuration. • **Top-Level Rule Set** — Opens the **Add New Top-Level Rule Set** window for adding a rule set at the top level of the rule sets tree. • (**Log Handler** is selected) — Lets you select **Log Handler** from a menu as the only accessible item to open the **Add New Log Handler** window for adding a new Log Handler rule set. • (**Error Handler** is selected) — Lets you select **Error Handler** from a menu as the only accessible item to open the **Add New Error Handler** window for adding a new Error Handler rule set . • (**User-Defined Property** is selected) — Lets you select **User-Defined Property** to open the **Add New User-Defined Property** window for adding a property.
Export	Opens the **Export Rule Set** window for exporting a rule set to the library or into a file.
Edit	Opens the **Edit Rule Set** window for editing a selected rule set.
Delete	Deletes a selected rule set. A window opens to let you confirm the deletion.
Move up	Moves a rule set up among other rules sets on the same level.
Move down	Moves a rule set down among other rule sets on the same level.
Move out of	Moves a rule out of its nesting rule set and onto the same level as the nesting rule set.
Move into	Moves a rule set out of its nesting rule set and into the rule set following this rule set.
Expand all	Expands all collapsed items on the rule sets tree.
Collapse all	Lets all expanded items on the rule sets tree collapse.

Rules toolbar

The rules toolbar provides the following options.

Table 4-7 Rules toolbar

Option	Definition
Add	Opens the **Add Rule** window for adding a rule.
Edit	Opens the **Edit Rule** window for editing a selected rule.
Delete	Deletes a selected rule. A window opens to let you confirm the deletion.
Move up	Moves a rule up within its rule set.
Move down	Moves a rule down within its rule set.
Copy	Copies a selected rule.
Paste	Pastes a copied rule.
Show details	Shows (or hides) details of a rule entry including the criteria.

Create a rule

Creating a rule includes several activities that are related to the different elements of a rule.

The **Add Rule** window is provided for creating a rule. It allows you to complete the activities for configuring the rule elements in the order that you prefer.

You can, for example, begin with naming and enabling a rule and then add the criteria, the action, and an event.

Tasks

- *Name and enable a rule* on page 62
  Configure name and enabling as general settings for a rule.
- *Add the rule criteria* on page 64
  Add the rule criteria to determine when a rule is applied.
- *Add the rule action* on page 66
  Add the action that is executed if the rule criteria matches.
- *Add a rule event* on page 67
  Optionally add one or more events that are executed if the rule criteria matches.

See also
Working with the Add Criteria window on page 62

Name and enable a rule

Configure name and enabling as general settings for a rule.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, select a rule set for the new rule.
3. Click **Add Rule** above the settings pane.

   The **Add Rule** window opens with the **Name** step selected.
4. Configure general settings for the rule:
   - **a** In the **Name** field, type a name for the rule.
   - **b** Select **Enable rule** to let the rule be processed when its rule set is processed.
   - **c** [Optional] In the **Comment** field, type a plain-text comment on the rule.

   Continue with adding the rule elements.

Working with the Add Criteria window

The window for adding the rule criteria provides several functions to help you with selecting suitable criteria elements.

According to the three elements of the rule criteria, the window is divided into the following columns:

- Left column for selecting a property
- Middle column for selecting an operator
- Right column for selecting an operand

Within a column, properties, operators, and operands are displayed in lists.

For example, you can select the following:

- Left column: *MediaType.EnsuredTypes*
- Middle column: *none in list*
- Right column: *Anti-Malware Media Type Whitelist*

This creates the criteria *MediaType.EnsuredTypes none in list Anti-Malware Media Type Whitelist*. If you add *Block* as the action, you get a rule for blocking access to media of all types that have not been entered in the specified whitelist.

To help you make suitable selections, the window does the following:

- Filters lists according to the filter settings that you provide
- Adapts lists in other columns when you select an item in one column to show only items that are suitable for being configured with the selected item
- Groups lists items in the left and right columns into the categories **Recommended**, **Suggested**, and **Other** if this categorization is possible for the currently displayed items
- Preselects two or three items (one per column) if they can be recommended for being combined with each other

Beginning with the left or right column

You can begin by selecting an item from the left or right column, depending on what you have already in mind about the criteria you are going to add.

For example, if this criteria is to be part of a rule for filtering infected web objects, you might begin by selecting the property *Antimalware.Infected* from the left column and then see what are suitable items to go with it. The result could be: *Antimalware.Infected* (property) *equals* (operator) *true* (operand).

On the other hand, if you want to include the criteria in a rule that prevents the users of your network from accessing drug-selling web sites, you might begin by selecting the URL category list *Drugs* as an operand and then combine it with a suitable operator and property. The result could be: *URL.Categories* (property) *at least one in list* (operator) *Drugs* (operand).

Left column

The list in the left column of the window allows you to select a property. The currently selected property appears at the top of the column in the **Selected property** field.

You can adapt the list in the following ways:

- Filter the list.
  - Using the **Filter** menu to filter according to:
    - Property type
    - Module (or *engine*) that is called to deliver a value for a property
    - Criteria group, such as Anti-Malware criteria, Media Type criteria, and others

      > This part of the menu appears also immediately before the window opens. After selecting a criteria group, the lists in all columns show only items that are suitable for configuring criteria of the selected group.

    - User-defined properties (to show only those properties)

  - Using a filtering term that you type in the input field below the menu
- Add self-configured properties to the list using the **Add User-Defined Property** button and window.

The list is automatically adapted when you select an operand from the list in the right column. Then it shows only properties that are suitable for being configured with this operand.

After selecting a property, you can configure its settings and parameters if it has any. The **Settings** and **Parameter** buttons are then displayed with the property, which open windows for configuring the respective items.

Middle column

The list in the middle column of the window allows you to select an operator. The currently selected operator appears at the top of the column in the **Selected operator** field.

The list is automatically adapted when you select an item from the list in the left or right column. Then it shows only operators that are suitable for being configured with the selected item.

Right column

The list in the right column of the window allows you to select an operand. The currently selected operand appears at the top of the column in the **Compare with** field.

An operand can be a single item of different types, a list of items, or another property. Types for single operands include Boolean, String, Number, Category, and others.

You can adapt the list in the following ways:

- Select an operand type (including the list and property types) from the list at the top of the column.

  Only items of this type are then displayed in the main list.

- (Only for lists and properties:) Filter the list using the **Filter** drop-down menu or the input field below .

If lists are displayed as operands, the **Add <list type>** and **Edit <list type>** buttons are provided at the bottom of the column. They open windows for adding and editing lists in the usual way.

The list is automatically adapted when you select a property from the list in the left column. Then it shows only operands that are suitable for being configured with this property.

Add the rule criteria

Add the rule criteria to determine when a rule is applied.

Task

1. In the **Add Rule** window, click **Rule Criteria**.
2. In the **Apply this rule** section, select when the rule is applied:
   - **Always** — The rule is always applied.

     Continue with adding another element, for example, the rule action.

   - **If the following criteria is matched** — The rule is applied if the configured criteria is matched.

     Continue with the next step.

3. In the **Criteria** section, click **Add** and select a criteria group from the drop-down menu.

The **Add Criteria** window opens displaying items that are suitable for configuring criteria from the selected group.

> ℹ To display items for all criteria, select **Advanced criteria**.

The window has three columns:

- Left column for selecting a property
- Middle column for selecting an operator
- Right column for selecting an operand

The currently selected elements are displayed at the top of each column under **Selected property**, **Selected operator**, and **Compare with**.

The window supports you in selecting suitable elements by automatically adapting the lists in the other columns after you have selected an item in one column. Then the other columns show only items that are suitable for being configured with the selected item.

You can begin by selecting an item from the left or right column. Accordingly, steps 4 to 6 could also be completed in a different order.

> ℹ If your criteria is to use a list as an operand, we recommend that you begin with selecting this list from the right column.

4 Select a property.

a From the list in the left column, select an item or leave the one that is preselected (if there is any).

> ℹ You can filter the list and add self-configured properties.

b [Conditional] If you have selected a property that requires settings, select settings from the **Settings** drop-down menu that is displayed with the property or leave the preconfigured settings.

c [Conditional] If you have selected a property that requires the setting of parameters, click **Parameters** below the property name and work with the options in the window that opens to set values for all required parameters.

5 Select an operator from the list in the middle column or leave the one that is preselected (if there is any).

6 Select an operand from the list in the right column or leave the one that is preselected (if there is any). If the list is empty, type a suitable value, for example, a number.

> To change the type of operands that are displayed, select a type from the list at the top of the column.

After selecting an individual operand or a type of operands, the lists in the middle and left columns are adapted to show suitable operators and properties.

7 Click **OK** to close the **Add Criteria** window.

The new criteria appears in the **Add Rule** window.

If you want to configure complex criteria, repeat steps 3 to 6 to configure more criteria parts.

Connect criteria parts by **AND** or **OR**, which are then provided as options. For three or more criteria parts, type parentheses to indicate how they are logically connected in the **Criteria combination** field, which appears then.

Continue with adding another element, for example, the rule action.

See also

Working with the Add Criteria window on page 62

Add the rule action

Add the action that is executed if the rule criteria matches.

Task

1 In the **Add Rule** window, click **Action**.

2 From the **Action** list, select one of the following actions:

- **Continue** — Continues with processing the next rule
- **Block** — Blocks access to an object and stops processing rules
- **Redirect** — Redirects the client that requested access to an object to another object
- **Authenticate** — Stops processing the current cycle and sends an authentication request
- **Stop Rule Set** — Stops processing the current rule set and continues with the next rule set
- **Stop Cycle** — Stops processing the current cycle, but does not block access to the requested object
- **Remove** — Removes the requested object and stops processing the current cycle

3 [Conditional] If you have selected an action that requires settings (Block, Redirect, Authenticate), select settings from the **Settings** list.

> Click **Add** or **Edit** before selecting settings to open windows for adding new settings or editing existing settings.

4 If you have created all required rule elements, but do not want to add an event:

a [Optional] Click **Summary** to review what you have configured.

b Click **Finish**.

The **Add Rule** window closes and the new rule appears within the rule set you have selected for it.

Add a rule event

Optionally add one or more events that are executed if the rule criteria matches.

Task

1. In the **Add Rule** window, click **Events**.
2. In the **Events** section, click **Add** and select **Events** from the drop-down menu.

   The **Add Event** window opens.
3. From the **Event** list, select an event.

   > To filter the list, type a filtering term in the input field above the list.
4. [Conditional] If you have selected an event that requires settings, select settings from the **Settings** list.

   > Click **Add** or **Edit** before selecting settings to open windows for adding new settings or for editing existing settings.
5. [Conditional] If you have selected an event that requires the setting of parameters, click **Parameters** and work with the options in the window that opens to set values for all required parameters.
6. Click **OK**.

   The **Add Event** window closes and the new event appears in the **Events** list.
7. If this is the last of the adding procedures:
   a. [Optional] Click **Summary** to review what you have configured.
   b. Click **Finish**.

      The **Add Rule** window closes and the new rule appears within the rule set you have selected for it.

Create a rule set

You can create a rule set and add it to your configuration.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, navigate to the position where you want to insert the new rule set.
3. Click **Add** above the rule sets tree.

   A drop-down menu opens.
4. Select **Rule Set**.

   The **Add New Rule Set** window opens.
5. Configure the following general settings for the rule set:
   - **Name** — Name of the rule
   - **Enable** — When selected, the rule set is enabled.
   - [Optional] **Comment** — Plain-text comment on the rule set

6 In the **Applies to** section, configure the processing cycles. You can select only one cycle, or any combination of these three:

- **Requests** — The rule set is processed when requests from the users of your network are received on the appliance.
- **Responses** — The rule set is processed when responses from web servers are received.
- **Embedded objects** — The rule set is processed for embedded objects sent with requests and responses.

7 In the **Apply this rule set** section, configure when the rule set is applied:

- **Always** — The rule set is always applied.
- **If the following criteria is matched** — The rule set is applied if the criteria configured below is matched.

8 In the **Criteria** section, click **Add**.

The **Add Criteria** window opens.

9 In the **Property** area, use the following items to configure a property:

- **Property** — List for selecting a property (property types shown in brackets)
- **Search** — Opens the **Property Search** window to let you search for a property.
- **Parameter** — Opens the **Property Parameters** window for adding up to three parameters, see Step 10.

  The icon is grayed out if the property has no parameters.
- **Settings** — List for selecting the settings of the module that delivers a value for the property (module names shown in brackets)

  The icon is grayed out if no settings are required for the property and *(not needed)* is added.
  - **Add** (String, Boolean, or numerical) — Configure it in the **Value** area. Then click **OK**.
  - **Edit** — Opens the **Edit Settings** window for editing the selected settings.

If no parameters need to be configured for the property, click **OK** and continue with Step 11.

10 If you need to add property parameters:

a Click **Parameter**.

The **Property Parameters** window opens.

b Add as many parameters as needed.

A parameter can be a:

- **Value** (String, Boolean, or numerical) — Configure it in the **Value** area. Then click **OK**.
- **Property** — Follow the instructions for editing properties, beginning with Step 4.

11 From the **Operator** list, select an operator.

12 In the **Parameter** area, add a parameter (also known as operand).

This can be a:

- **Value** (String, Boolean, or numerical) — Configure it in the **Value** area.
- **Property** — Follow the instructions for editing properties, beginning with Step 4.

13 Click **OK** to close the **Add Criteria** window.

14 [Optional] Click the **Permissions** tab and configure who is allowed to access the new rule set.

15 Click **OK**. to close the **Add New Rule Set** window.

The **Add New Rule Set** window closes and the rule set is inserted into your rule set system.

16 Click **Save Changes**.

Import a rule set

You can import a rule set from the library into your rule set system.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, navigate to the position where you want to insert the new rule set.

3 From the **Add** drop-down menu, select **Rule Set from Library**.

A window with a list of the library rule sets opens.

4 Select the rule set you want to import, for example, the **Gateway Antimalware** rule set.

If conflicts arise when importing this rule set, they are displayed in the window.

> Conflicts arise when a rule set uses configuration objects, such as lists or settings, that already exist in your rule set system.

5 Use one of the following methods to solve conflicts:

- Click **Auto-Solve Conflicts** and choose one of the following strategies for all conflicts:
  - **Solve by referring to the existing objects** — If rules of the imported rule set refer to objects existing in the appliance configuration under the same names, references are made to apply to these existing objects.
  - **Solve by copying and renaming to suggested** — If rules of the imported rule set refer to objects existing in the appliance configuration under the same names, these objects are also used, but are renamed, so as to avoid conflicts.
- Click the listed conflicts one after another and solve them individually by choosing either of the two above strategies each time.

6 Click **OK**.

The rule set is inserted in the rule sets tree. It is enabled by default.

List and settings that the rule set needs to perform its filtering job are implemented with the rule set and can be viewed on the lists and settings trees.

7 If necessary, use the blue arrows above the rule sets tree, to move the rule set to where you want it to be.

8 Click **Save Changes**.

Restrict access to configuration items

When creating rule sets, lists, or settings, or working with existing ones, you can restrict access to them.

Task

1 Select **Policy** | **Rule Sets** (or **Lists** or **Settings**).

2 On the tree structure, navigate to the position where you want to add the new item.

3 Click **Add** above the tree structure.

An **Add** window opens.

4 Complete the steps for adding a new item. Then click the **Permissions** tab.

Three modes of access can be configured: *Read and Write*, *Read*, and *No Access*.

5 Click **Add** under the **Read and Write** pane.

The **Add Role or User** window opens.

6 Select a role or a user (or more than one of each type at once) from the list in the corresponding pane. Or type a wildcard expression as the name of a role or user in the **Wildcard** field.

7 Add as many entries to the **Read and Write** list as needed.

Use the **Delete** button under the pane to delete entries

8 Fill the **Read** and **No Access** panes in the same way.

9 Use the radio buttons under **All other roles have** to configure access for all roles and users that are not included in one of the lists on the tab.

10 Click **OK** to close the window.

11 Click **Save Changes**

5 Lists

Lists are used by rules or retrieving information on web objects and users.

There are several types of lists, which differ, for example, with regard to who created them or which type of elements they contain. Accordingly, you work with these lists in different ways.

Lists appear in different places on the user interface, for example, in the criteria of rules and rule sets, on the Lists tab, and within settings.

At the initial setup of the appliance, lists are implemented together with the rule set system.

You can then review the lists of the implemented system, modify and delete them, and also create your own lists.

Contents

List types

Web security rules use several types of lists for retrieving information on web objects and users.

There are the following types of lists on the appliance:

- **Custom lists** — These lists can be modified by you. They are displayed on the upper branch of the lists tree on the **Lists** tab.

  Custom lists include string, number, category, and other types of lists. Different list types can require different methods of maintaining them.

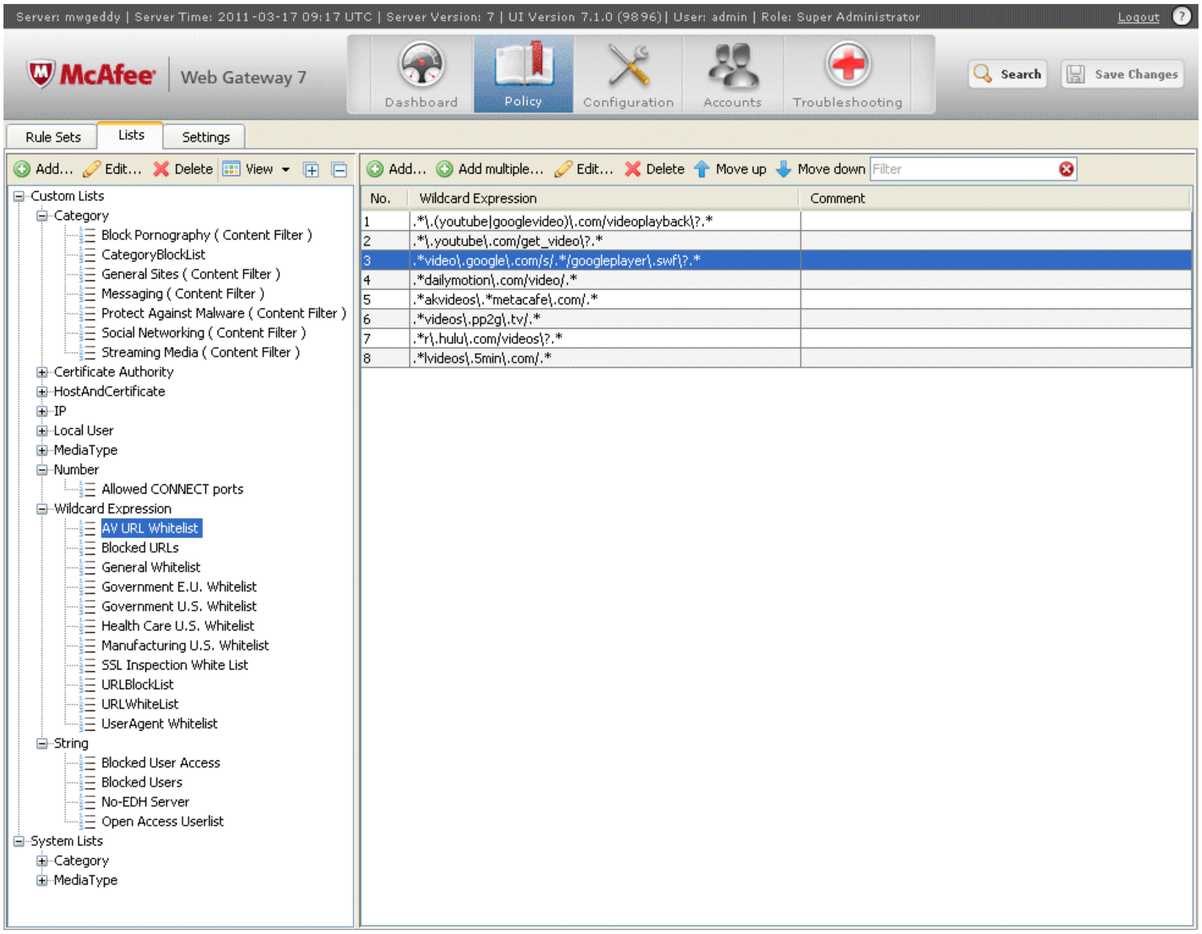
- **System lists** — These lists cannot be modified. They are displayed on the lower branch of the lists tree on the **Lists** tab.

  System lists include category and media type lists.

- **Inline lists** — These lists can also be modified, but they do not appear on the **Lists** tab. They appear “inline” as part of the settings of a configuration item, for example, as part of the settings of a network protocol.

Lists tab

The **Lists** tab allows you to work with lists.



Server: mwgeddy | Server Time: 2011-03-17 09:17 UTC | Server Version: 7 | UI Version 7.1.0 (9896) | User: admin | Role: Super Administrator

- Custom Lists
  - Category
    - Block Pornography (Content Filter)
    - CategoryBlockList
    - General Sites (Content Filter)
    - Messaging (Content Filter)
    - Protect Against Malware (Content Filter)
    - Social Networking (Content Filter)
    - Streaming Media (Content Filter)
  - Certificate Authority
  - HostAndCertificate
  - IP
  - Local User
  - MediaType
  - Number
    - Allowed CONNECT ports
  - Wildcard Expression
    - AV URL Whitelist
    - Blocked URLs
    - General Whitelist
    - Government E.U. Whitelist
    - Government U.S. Whitelist
    - Health Care U.S. Whitelist
    - Manufacturing U.S. Whitelist
    - SSL Inspection White List
    - URLBlockList
    - URLWhiteList
    - UserAgent Whitelist
  - String
    - Blocked User Access
    - Blocked Users
    - No-EDH Server
    - Open Access Userlist
- System Lists
  - Category
  - MediaType

No.	Wildcard Expression	Comment
1	.*\.(youtube|googlevideo)\.com/videoplayback\?.*	
2	.*\.youtube\.com/get_video\?.*	
3	.*video\.google\.com/s/.*/googleplayer\.swf\?.*	
4	.*dailymotion\.com/video/.*	
5	.*akvideos\.*metacafe\.com/.*	
6	.*videos\.pp2g\.tv/.*	
7	.*r\.hulu\.com/videos\?.*	
8	.*lvideos\.5min\.com/.*	

Main elements of the Lists tab

The following table describes the main elements of the **Lists** tab.

Table 5-1 Main elements of the Lists tab

Element	Description
Lists toolbar	Items for working with the lists on the lists tree
Lists tree	Tree structure displaying the lists of the appliance configuration
List entries toolbar	Settings of the currently selected item on the settings tree
List entries	Entries of the currently selected list

Lists toolbar

The lists toolbar provides the following options.

Table 5-2 Lists toolbar

Option	Definition
Add	Opens the **Add List** window for adding a list.
Edit	Opens the **Edit List** window for editing a selected list .

Table 5-2 Lists toolbar *(continued)*

Option	Definition
Delete	Deletes a selected list. A window opens to let you confirm the deletion
View	Opens a menu to let you display the lists in different ways (A-Z, Z-A, by list type, with or without list types for which currently no lists exist).
Expand all	Expands all collapsed items on the lists tree.
Collapse all	Lets all expanded items on the lists tree collapse.

List entries toolbar

The list entries toolbar provides the following options.

Table 5-3 Lists entries toolbar

Option	Definition
Add	Opens the **Add <List type>** window for adding a list entry, for example, the **Add String** window.
Add multiple	Opens the **Add <List type>** window for adding multiple list entries if this is possible for a list type.
Edit	Opens the **Edit <List type>** window for editing a selected list entry, for example, the **Edit String** window.
Delete	Deletes a selected list entry. A window opens to let you confirm the deletion.
Move up	Moves an entry up the list.
Move down	Moves an entry down the list.
Filter	Input field for typing a filtering term to display only matching list entries ℹ The filtering function works as soon as you type a character in the field.

Access a list

You can access a list on the **Lists** tab or by clicking a list name in a rule.

Tasks

- *Access a list on the Lists tab* on page 74
  To access a list on the **Lists** tab, you locate it on the lists tree and select the list.
- *Access a list in a rule* on page 74
  To access a list in a rule, you locate the rule on the **Rule Sets** tab and click the list name.

Access a list on the Lists tab

To access a list on the **Lists** tab, you locate it on the lists tree and select the list.

Task

1. Select **Policy** | **Lists**
2. On the lists tree, navigate to the branch that contains the list you want to access and click the list name.

   The list entries appear on the settings pane.

You can now work with the list.

Access a list in a rule

To access a list in a rule, you locate the rule on the **Rule Sets** tab and click the list name.

Task

1. Select **Policy** | **Rule Sets**
2. On the rule sets tree, select the rule set that contains the rule with the list you want to access.

   The rules of the rule set appear on the settings pane.
3. Make sure **Show details** is selected.
4. In the rule with the list you want to access, do one of the following:
   - Click the list name in the rule name if it is contained in this name.
   - Click the list name in the rule criteria.

   An **Edit List <Type>** window opens, where <*Type*> is the type of the list you are accessing.

You can now work with the list.

Create a list

You can create lists of your own in addition to those that were implemented on the appliance at the initial setup or when you imported a list from the library.

Creating a list includes the following two steps:

- Adding a new list
- Filling the new list with entries

Tasks

- *Add a new list* on page 75
  You can add a new list that you fill with entries later.
- *Fill a list with entries* on page 75
  When you have added a new list on the appliance, you need to fill it with entries.

Add a new list

You can add a new list that you fill with entries later.

Task

1 Select **Policy** | **Lists**.

2 On the lists tree, navigate to the position where you want to add the list.

3 Click **Add** on the toolbar.

The **Add List** window opens, with the **Add List** tab selected.

4 Use the following items to configure general settings for the list:

- **Name** — Name of the list
- **Comment** — [Optional] Plain-text comment on the list
- **Type** — List for selecting a list type

5 [Optional] Click the **Permissions** tab and configure who is allowed to access the list.

6 Click **OK**.

The **Add List** window closes and the new list appears on the lists tree.

7 Click **Save Changes**.

You can now fill the list with entries.

Fill a list with entries

When you have added a new list on the appliance, you need to fill it with entries.

Task

1 Select **Policy** | **Lists**.

2 From the lists tree, select the list you want to add entries to.

3 Click **Add** on the settings pane.

The **Add <List type>** window opens, for example, the **Add String** window.

4 Add an entry in the way it is done for a particular list type.

5 [Optional] In the **Comment** field, type a plain-text comment on the list entry.

6 Click **OK**.

The **Add <List type>** window closes and the entry appears in the list.

7 Click **Save Changes**.

See also

Work with different types of lists on page 76

Work with different types of lists

Working with lists is done differently depending on the list type.

For example, if the type is *String*, you can add entries by typing strings in the **String** field of the **Add String** window. However, if the type is *MediaType*, you need to select an entry from a media type folder, which is part of a system of folders.

For string and wildcard expression lists, there is the option to add multiple entries at once by clicking Add multiple and typing text for each entry in a new line.

For media type lists, you can select multiple entries or folders at once if you do not want to add them separately.

Tasks

- *Add a wildcard expression to a global whitelist for URLs* on page 76
  You can add a wildcard expression to a whitelist used by a global whitelisting rule.
- *Add a URL category to a blocking list* on page 77
  You can add a URL category to a blocking list to block access to all URLs falling into that category.
- *Add a media type to a media type filter list* on page 77
  You can add a media type to a list for media type filtering.

Add a wildcard expression to a global whitelist for URLs

You can add a wildcard expression to a whitelist used by a global whitelisting rule.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, select a rule set that contains rules for global whitelisting, for example **Global Whitelist**.

   The rules appear on the settings pane.
3. Find the rule that uses a whitelist to exempt requests when they submit URLs for hosts matching the wildcard expressions on the list, for example, **URL.Host matches in list Global Whitelist** and click on the list name.

   ℹ A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

   The **Edit List (Wildcard Expression)** window opens.
4. Click **Add**.

   The **Add Wildcard Expression** window opens.
5. In the **Wildcard expression** field, type a wildcard expression.

   To add multiple wildcard expressions at once, click **Add multiple** and type every wildcard expression in a new line.
6. [Optional] In the **Comment** field, type a comment on the wildcard expression.
7. Click **OK**.

   The window closes and the wildcard expression appears on the whitelist.
8. Click **Save Changes**.

Add a URL category to a blocking list

You can add a URL category to a blocking list to block access to all URLs falling into that category.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select the rule set that contains rules for URL filtering.

   The rules appear on the settings pane.

3 Find the rule that uses a category blocking list, for example, **Block URLs whose category is in Category BlockList**, and click on the list name.

   > A yellow triangle next to the list means that the list is initially empty and you need to fill the entries.

   The **Edit List (Category)** window opens.

4 Expand the group folder with the category you want block, for example, **Purchasing**, and select the category, for example, **Online Shopping**.

   To add multiple categories at once, select multiple categories or one or multiple group folders.

5 Click **OK**.

   The window closes and the category appears on the blocking list.

6 Click **Save Changes**.

Add a media type to a media type filter list

You can add a media type to a list for media type filtering.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, navigate to a rule set that contains rules for media filtering, for example, the nested **Download Media Types** rule set of the Media Type Filtering rule set and select it.

   The rules appear on the settings pane.

3 Select the rule **Block types from Media Type Blocklist** and click on the list name.

   The **Edit List (MediaType)** window opens.

4 Click **Edit**.

   An **Edit** window opens. It displays a list of group folders with media types.

5 Expand the group folder with the media type you want to add, for example, **Audio**, and select the media type, for example, **audio/mp4**.

   To add multiple media types at once, select multiple media types or one or multiple group folders.

6 Click **OK**.

   The window closes and the media type appears on the filter list.

7 Click **Save Changes**.

External lists

Data can be retrieved from external sources, for example, web servers, and used in rules on the appliance.

This data can be a complete list or a single value. It is generally referred to as *external lists* or *external list data*. Different data types can be used in an external list, such as strings, numbers, IP addresses, and others.

An important feature of external lists is that they are processed dynamically on the appliance. All retrieving and conversion of external list data happens at run time when the data is first used in a rule.

When the data has been retrieved, it is stored in an internal cache for a period of time that you can configure, but not on disk, so it will not persist after a restart of the appliance. Also external lists do not appear on the lists tree of the user interface.

External lists properties

Access to data retrieved from external sources is provided through special properties. The name of an external list property is *ExtLists.<type>*, where *<type>* is the type of elements in the list that is the value of the property. For example, the value of *ExtLists.IntegerList* is a list of integers. Possible list element types include String, Number, Wildcard Expression, and others.

Usually the value of an external list property is a list, but there also external list properties for single values. When an external source delivers more than one value as input for the latter type of property, only the last value is retrieved and stored.

External list data can be filtered, depending on the source type, and converted into a different format, depending on the type of the property used in a given rule.

By configuring parameters for an external list property, you can specify placeholders that are substituted with property parameters at run time. Using these placeholders, you can let the content of an external list depend on criteria such as a user name or user group name.

For logging purposes, you can use the *ExtLists.LastUsedListName* property, which has as its value the name of the settings for the External Lists module that were used last.

External Lists module

To specify which data should be retrieved from an external source, you need to configure the settings of the *External Lists* module (also known as the External Lists filter or engine), which retrieves the data.

When external data cannot be retrieved successfully, the External Lists module returns an error code, which you can process using Error Handler rules. A separate range of error IDs is available for this purpose.

The External Lists module consumes memory for caching data that it retrieves from external sources. You should take this into account when setting up rules for external list handling.

Sources of external list data

The sources of the content that external lists are filled with can be the following:

- A web service, which is accessed under the HTTP, HTTPS, or FTP protocol
- A file within your local file system
- An LDAP or LDAPS server

- A database:
  - PostgreSQL
  - SQLite3

For performing queries on the databases, the SQL query language is used. However, the particular query format can be different for both database types.

As an SQLite3 database operates file-based, we recommend it for testing, rather than for production environments. However, you might still want to use it if you already have data in a database of this type. Otherwise it is easier to use Web Service or File data sources for retrieving external list content.

Recommended use

Working with the external lists feature is recommended in cases like the following.

You need to handle a large number of lists that are mostly stored in external sources, you are running multiple appliances as nodes in a Central Management configuration, and you need to apply frequent changes to the list data.

Synchronizing all list data on all nodes could then no longer be scalable.

Use of external list data in rules

To handle external list data, you need to configure rules that contain suitable external list properties in their criteria.

Suppose you want to block a request for a web object if its URL has a destination IP address that is within one of the IP address ranges on a list that is stored in an external source.

You can achieve this with the following rule:

Block URLs with IP addresses in forbidden range

URL.Destination.IP is in range ExtLists.IPRangeList(" ", " ", " ")<External Lists> –> Block<URL Blocked>

When the rule is processed, it is checked whether the IP address that is the value of the *URL.Destination.IP* property is within one of the ranges on the list that is the value of *ExtLists.IPRangeList*.

Together with the external list property, the *<External Lists>* settings are specified. These are the settings that the External Lists module uses to retrieve the appropriate data as the value for the external list property.

You need to configure these settings to let the module know where a particular external list should be retrieved from and how the retrieval is performed. For example, if this list is stored in a text file on a web server, you can specify the URL that allows access to the file.

Other information that you can configure as part of these settings includes timeouts and size limits.

The parameters of an external list property are optional. They are empty in this example.

By default, no rules for handling external lists exist on the appliance. If you want to use external list data to restrict web access for the users of your network, you need to set up one or more rules like the above and insert them into a suitable rule set.

Substitution and placeholders

To allow more flexibility in retrieving external list data, placeholders can be used when configuring the settings of the External Lists module, for example, in URLs.

A placeholder is substituted at run time with a value that you provide as a parameter of an external list property.

For example, you want to retrieve data from a web service that delivers lists of media types allowed for individual users. A URL for a particular media type list would then be:

`http://my-web-service.com/ mediatypes?user=` <value>

where <value> is the name of a user.

Configuring separate settings for the External Lists module to cover each user individually would be tiresome, so you can use a placeholder in the following way:

- For the *Web service's URL* parameter in the settings, you specify:

  ```
  http://my-web-service.com/mediatypes?user=${0}
  ```

  where `${0}` is a placeholder for the first of the three parameters of the external list property you are using in a rule.

- For the first parameter of the external list property, you specify the *Authentication.Username* property.

This retrieves a list with the media types that are allowed for an individual user. The user name is the one that this user submitted when required to authenticate after sending a request to access media of a particular type.

You can use the following two types of placeholders:

- *${<n>}* — Placeholder that is substituted with a converted value

  <n> is the position number (0, 1, 2) for a parameter of an external list property. At run time, this placeholder is substituted by the value that you specified when configuring the parameter.

  Before the placeholder is substituted, the value is converted. This process is also known as "escaping". The conversion is performed according to the internal rules of the data source that is involved.

  For example, if the source is a web service, it replaces all characters that are not allowed by *%XX* sequences, as is specified in the corresponding HTTP standard (RFC 2616).

- *$<<n>>* — Placeholder that is substituted with a non-converted value

  As above, but without conversion. This means you need to ensure yourself that the substitution does not lead to unwanted results.

  You can use this type of placeholder when complete URLs, rather than parts of them are to be substituted.

Configure the External Lists module

You can configure settings for the External Lists module to provide the information the module needs to retrieve external list data.

By default, no settings exist for this module on the appliance. You need to add individual settings and configure them for each external list you want to retrieve data from in a rule.

Task

1 Select **Policy** | **Settings**.

2 On the settings tree, select **External Lists** and click **Add**.

The **Add Settings** window opens.

3 In the **Name** field, type the settings name.

4 [Optional] In the **Comment** field, type a plain-text comment on the settings.

5 [Optional] Click the **Permissions** tab and configure who is allowed to access the settings.

6 Configure the other settings parameters as needed.

7 Click **OK**.

The window closes and the settings appear under **External Lists** on the settings tree.

8 Click **Save Changes**.

See also
External Lists module settings on page 81

External Lists module settings

The External Lists module settings are used to configure the module that retrieves data from external sources.

Data Source Type

Settings for the type of source that data is retrieved from

You can configure specific settings for each source type in another section, which appears depending on what you select here.

Table 5-4 Data Source Type

Option	Definition
Web service	Data is retrieved using a web service under the HTTP, HTTPS, or FTP protocol.
File on disk	Data is retrieved from a file within your local file system.
LDAP	Data is retrieved from an LDAP server.
Database	Data is retrieved from a PostgreSQL or SQLite3 database.

Common Parameters

Settings for time limits in handling external lists

Table 5-5 Common Parameters

Option	Definition
Operation timeout	Time (in seconds) to elapse before an operation for handling external lists is aborted if it cannot be completed successfully This option applies when the source of an external list is a web server. The timeout is reached, for example, when a web server does not respond to a request from the appliance. You can specify the expiration of the timeout as: • **Simple expiration** — When selected, you can specify the time (in minutes) to elapse before retrieved list data is removed from the internal cache in the Expiration time input field • **Scheduled expiration** — When selected, you can specify the time that is to elapse before an external list is removed from the internal cache in several input fields that appear
Expiration time	Time (in minutes) to elapse before retrieved data is removed from the internal cache
Minutes/Hours/ Days/Months/ Week days	Time to elapse before retrieved data is removed from the internal cache These input fields appear when you select *Scheduled expiration*. Your input must be in a "cron"-compliant format because the removal is calculated and performed by a cron job. For more information, see the *crontab (5)* man page of the documentation for Linux (UNIX) operating systems. You can specify values in one of these fields or in any combination of fields.

Data Conversion Settings

Settings for converting data that is retrieved from an external source

These settings are only available when you have selected **Web service** or **File on disk** as the source of the data.

Table 5-6 Data Conversion Settings

Option	Definition
Data type	List for selecting the input format of the data that is converted You can select one of the following: • **Plain text** — The data is in plain-text format Each line appears as a separate entry in a converted list. Optionally, you can specify a regular expression as a filtering term in the input field below. Only strings matching this term are then entered into the list. If there is no grouping operator in the regular expression, the complete string is stored in a list. Otherwise, the data captured by the first group is stored. • **XML** — The data is in XML format You need to specify an XPath expression to select the data that should be retrieved. Data could be retrieved, for example, according to XML tags or attributes.
Regular expression	Regular expression used for filtering converted data This option appears when you have selected **Plain text** under **Data type**.
XPath expression	XPath expression used for filtering converted data This option appears when you have selected **XML text** under **Data type**. For information on how to use XPath expressions, refer to appropriate documentation, for example, the XPath tutorial that is provided on the *w3schools* site.

Web Service Specific Parameters

Settings applying when the source of an external list is provided by a web service

These settings appear when Web service is selected in the **Data Source Type** section.

Table 5-7 Web Service Specific Parameters

Option	Definition
Web service's URL	URL of a file on a web server that contains an external list and is provided by a particular web service (HTTP, HTTPS, or FTP) You can specify a placeholder inside the URL.
Specify authentication data	When selected, you can specify information for an authentication that must be performed successfully before data can be retrieved from a web service
Type of HTTP authentication	List for selecting a type of HTTP authentication Supported types are: None, Basic, Digest
User's name	User name submitted for the authentication
User's password	Password submitted for the authentication Click **Set** to open a window for settings a password
Use next-hop proxy for access to server	When selected, access to the web server is achieved using a next-hop proxy server After selecting this checkbox, the following three items become accessible.
List of next-hop proxy servers to use	List for selecting a list of servers that can be used as next-hop proxies to access a web server Click **Add** or **Edit** to open windows for adding a new list or editing an existing list

Table 5-7 Web Service Specific Parameters *(continued)*

Option	Definition
List of certificate authorities	List for selecting a list of certificate authories that can be used in SSL-secured communication with a web service Click **Add** or **Edit** to open windows for adding a new list or editing an existing list
List of additional HTTP headers	List of headers that are added to an HTTP request that has been received on an appliance

The following table describes the elements of a entry in the **List of additional HTTP headers**.

Table 5-8 Additional HTTP headers – List entry

Option	Definition
Header name	Name of a header that is added to an HTTP request
Header value	Value of a header that is added to an HTTP request
Comment	Plain-text comment on a header

File Specific Parameters

Settings applying when the source of an external list is a file within your local file system

These settings appear when **File on disk** is selected in the **Data Source Type** section.

Table 5-9 File Specific Parameters

Option	Definition
File name	Name of the file from your local file system that is the source of an external list You can specify a placeholder inside the URL. To restrict the possible location of the file, you can specify a part of your local file system when configuring the External Lists system settings. The file must be within the specified part then, for example, *opt/mwg/temp*.

LDAP Specific Parameters

Settings applying when the source of an external list is an LDAP server

These settings appear when **LDAP** is selected in the **Data Source Type** section.

Table 5-10 LDAP Specific Parameters

Option	Definition
LDAP server's URL	Name of the file from your local file system that is the source of an external list You can specify a placeholder inside the URL. To restrict the possible location of the file, you can specify a part of your local file system when configuring the External Lists system settings. The file must be within the specified part then, for example, *opt/mwg/temp*.
List of certificate authorities	List for selecting a list of certificate authories that can be used in SSL-secured communication with a web service Click **Add** or **Edit** to open windows for adding a new list or editing an existing list
User name	User name the appliance submits when attempting to connect to the LDAP server

Table 5-10 LDAP Specific Parameters *(continued)*

Option	Definition
LDAP password	Password the appliance submits when attempting to connect to the LDAP server You can set or change the password using the **Set/Change** toggle button that is provided.
Search DN	Name of a domain in the database on an LDAP server that is searched for an external list You can specify a placeholder inside this name.
Search scope	List for selecting the scope of the search for an external list on an LDAP server • **Subtree** — The complete subtree of the domain specified under **Search DN** is searched. • **One level** — Only one level below the domain specified under **Search DN** is searched. • **Base** — Only the base of the domain specified under **Search DN** is searched.
Search filter	Term for filtering the results of the search for an external list on an LDAP Only if the name of an entry in the database matches the filtering term, the item that the entry represents is retrieved. You can specify a placeholder within this term.
Attribute	Attribute of an item in the database on an LDAP server that is the intended search result, for example, an email address
Enable LDAP version 3	When selected, version 3 of the LDAP protocol is used If you disable this option, you need to provide the encoding that is used for communication with the LDAP server. The following input field for this information appears when you deselect **Enable LDAP version 3**.
Allow LDAP library to follow referrals	When selected, referrals to locations outside the LDAP server that a search for an external list performed on can be followed to retrieve the list

Database Specific Parameters

Settings applying when the source of an external list is a database

These settings appear when **Database** is selected in the **Data Source Type** section.

Table 5-11 Database Specific Parameters

Option	Definition
SQL query	String denoting the type of query that is performed on a database The default type of query used for retrieving external lists information is SELECT. You can put a *;* (semicolon) at the end of the string, but this is not required. A query can also use placeholders to include variable data. If the *$N* placeholder is used, the data that is filled in as the value of the variable is "escaped" to prevent an SQL injection. Then a \ (backslash) is replaced with \\ (double backslash), and and an ' (apostrophe) with a \ (backslash). An SQL query usually returns one data column. if you perform a query that returns multiple columns, only the first is used for external list content. To retrieve content from several columns, you need to specify combined columns for output, using appropriate SQL operators.
Type of database	Type of database that external list content is retrieved from The following two types are available: • PostgreSQL • SQLite3 After selecting a database type, database specific parameters appear according to this type.

Table 5-12 PostgreSQL Database Specific Parameters

Option	Definition
Database host	Host name of the server that the database resides on
Database port	Port number of the port on the database host that listens to queries for retrieving external list content The default port number is 5432.
Name of database on database server	Name the database is known under on the database server
Database user name	User name of an appliance when connecting to the database server
Database password	Password for the user name of the appliance The **Set** button opens a window for setting the password.

Table 5-13 SQLite Database Specific Parameter

Option	Definition
File path to SQLite database	Full path to the file on an appliance that contains the database

Advanced Parameters

Settings for advanced methods of handling external lists

Table 5-14 Advanced Parameters

Option	Definition
Skip "bad" entries during data conversion	When selected, data that cannot be converted to the required type, such as Integer, Double, or Boolean, is omitted
Maximal number of entries to fetch	Maximum number of entries that are retrieved from an external list The number can range from 0 to unlimited We recommend that you specify a limit here to avoid high memory consumption in case of large lists.
Maximal size of entries to fetch	Maximum amount of data (in KB): 0 to unlimited) that is retrieved from an external list The number can range from 0 to unlimited We recommend that you specify a limit here to avoid high memory consumption in case of large lists. This option is not available when the source of the external list is an LDAP server.

Configure general settings for external lists

You can configure settings applying to all external lists that are retrieved for use on the appliance.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to configure settings for and click **External Lists**.

The settings for the external lists appear on the settings pane.

3 Configure these settings as needed.

4 Click **Save Changes**.

See also

External Lists system settings on page 87

External Lists system settings

The External Lists system settings apply to all external lists that are processed on the appliance.

Global Configuration

Setting for the internal cache on the appliance that stores external list data

Table 5-15 Global Configuration

Option	Definition
Flush External Lists Cache	Removes the data that is stored in the internal cache
Time before retry after failure	Time (in seconds) that the External Lists module remembers a failure to retrieve data from a particular external source The module will not perform retries for a source as long as it remembers the failure. We recommend that you keep the default value or modify it according to the requirements of your network. This way you avoid adding load by constant retries to a web server that is already overloaded.

File Data Source Configuration

Setting for the local file system that external list data can be retrieved from

Table 5-16 File Data Source Configuration

Option	Definition
File system allowed for file data access	Path leading to the folder for storing external lists within your local file system External lists that data is retrieved from must be stored in this folder. Otherwise an attempt to retrieve the data will lead to an access-denied error. ℹ When external list data is retrieved from an SQLite database, the path specified here is the path to the folder within your local file system that contains the database.

Web Data Source Configuration

Setting for all web services that are the sources of external list data

Table 5-17 Web Data Source Configuration

Option	Definition
Check SSL certificate identity	When selected, a certificate that a web server submits in SSL-secured communication under the HTTPS protocol is verified The verification is performed according to the SSL scanning rules that are implemented on the appliance. This can, for example, lead to an error if the web server uses a self-signed certificate.

Subscribed lists

Lists for use in web security rules can be filled with content that is retrieved from suitable servers. These lists are known as subscribed lists.

When working with subscribed lists, you only have to configure general settings, such as the list name, yourself. For the list content, for example, IP addresses or URLs, you rely on a server, which can be the McAfee server that is provided for maintaining subscribed lists or another server that you specify.

Subscribed lists that retrieve their content from the McAfee server are known as *McAfee-maintained lists*. Lists that retrieve their content from another server are known as *customer-maintained lists*.

After you have created a subscribed list, it appears on the Subscribed Lists branch of the lists tree on the user interface. You can work with a subscribed list in the same way as with other lists on the lists tree.

> There is a restriction in size for subscribed lists. A subscribed list must not be larger than 4 MB or contain more than 100,000 entries.

By configuring update schedules or performing updates manually, you ensure that the latest content is made available to the web security rules by a subscribed list.

Retrieving list content from the McAfee server

When the content of a subscribed list is retrieved from the McAfee server that is provided for this purpose, you select the type of content for this list from a catalog.

The content is maintained on the McAfee server. To ensure that McAfee-maintained lists hold the latest content, you perform manual updates on the user interface of your appliance.

Retrieving list content from another server

When the content of a subscribed list is retrieved from a server other than the McAfee server, you specify the URL for the file that holds this content on the server.

The content is maintained on this server. Updates for this kind of subscribed lists are performed according to a schedule that you set up when configuring the list settings.

Create a subscribed list

To create a subscribed list, you configure general list settings and settings for the list content.

Task

1. Select **Policy** | **Lists**.
2. Above the lists tree, click the **Add** icon.

   The **Add List** window opens.
3. Configure general settings for the list.
   - a In the **Name** field, type the list name.
   - b From the **Type** lists, select the list type.
   - c Under **Contains**, select the type of entry that the list will contain.
   - d [Optional] In the **Comments** field, type a plain-text comment on the list.
   - e [Optional] Click the **Permissions** tab and configure who is allowed to access the list.
4. Select **List content is elsewhere**.

5 Configure settings for the list content.

- For list content that is retrieved from the McAfee server:
  - Under **Source**, select **McAfee maintained list**.
  - Click **Choose**.

    The **Choose List Content** window opens.
  - Select a content type
  - Click **OK** to close the window.
- For list content that is retrieved from another server:
  - Under **Source**, select **Customer maintained list**.
  - Click **Setup**.

    The **Setup** window opens.
  - Configure settings for the list content.
  - Click **OK** to close the window.

6 Click **OK** again.

The **Add List** window closes and the list appears on the **Subscribed Lists** branch of the lists tree.

7 Click **Save Changes**.

See also
Settings for subscribed lists content on page 91

Updating subscribed lists

Updates of subscribed lists content are performed manually or according to a schedule, depending on whether the content is retrieved from the McAfee server that is provided for this purpose or from another server.

For list content that is retrieved from the McAfee server, you must perform updates manually. Each time you perform a manual update, all McAfee-maintained lists are updated together.

The content of McAfee-maintained lists is also updated each time you create a new list of this kind.

For list content that is retrieved from a server other than the McAfee server, updates are performed according to a schedule. Each subscribed list has a schedule of its own. You can set up and modify the schedule when configuring the settings for the list content.

When administering subscribed lists on a node in a Central Management configuration, updates are shared by all other nodes within the update group.

The update group is configured in the section **This Node is a Member of the Following Groups** of the Central Management settings.

See also
Settings for subscribed lists content on page 91
Central Management settings on page 294

Update subscribed lists maintained on the McAfee server

For subscribed lists that are maintained on the McAfee server, you must perform updates manually.

The content of McAfee-maintained lists is also updated each time you create a new list.

Task

1 Select **Configuration** | **Appliances**.

2 On the toolbar above the appliances tree, click **Manual Engine Update**.

The content of all McAfee-maintained lists is updated.

Settings for subscribed lists content

When a subscribed list is maintained on a server other than the McAfee server, settings must be configured for its content.

Table 5-18 Settings for subscribed list content

Option	Definition
URL to download	URL of a file with content for a subscribed list The format for specifying the URL is: `HTTP` | `HTTPS` | `FTP ://`<path>`/`<filename>`.`<extension>
Use this	When selected, the certificate contained in the certificate authority chain appearing next to the radio button is used. This is required if the connection to the server that provides the list content is a SSL-secured connection for communication under the HTTPS protocol.
Ignore certificate errors	When selected, certificate errors will not cause a failure to retrieve a list content from a server
URL authentication	Section for configuring a user name and password if authentication is required for access to a server • **User name** — User name for authenticating to the server • **Password** — Password for authenticating to the server
Proxy	List of proxy servers that can be used for accessing a server that provides list content By default, no proxy server is used to access a list content server.
Add Proxy	Opens a window for adding a proxy server to the list.
List content update	Section for configuring an update schedule for list content An update can be performed: • **Hourly at** — Minutes after the full hour • **Daily at** — Hours and minutes • **Weekly at** — Day of the week with hours and minutes • **Every** — Minutes of the interval that is to elapse before the next update

Common Catalog

The Common Catalog provides lists that can be pushed from a McAfee ePO server to an appliance. A REST (Representational State Transfer) interface runs internally on both systems to enable the transfer of the list data. A McAfee ePO extension must also be installed and running on the appliance.

You must set up a user account, as there must be an instance on the appliance that is allowed to handle the transfer of the list data. You can set up the account using the **ePO Orchestrator** settings.

After lists from the Common Catalog have been pushed to an appliance, they appear on the **Lists** tab of its user interface. A prefix in the list name indicates that a McAfee ePO server is the source of a list.

You can use these lists to configure rules like any other lists on the **Lists** tab.

The following types of lists can be pushed:

- IP address
- Domain name
- String
- Wildcard expression

Set up a user account for Common Catalog lists

To enable the use of Common Catalog lists on an appliance, you must set up a user account to create an instance that is allowed to handle the transfer of the list data.

Task

1. Select **Configuration | ePolicy Orchestrator.**
2. Under **ePolicy Orchestrator Settings**, configure a user account.
   a. In the **ePO user account** field, type a user name or leave the preconfigured value, which is `ePO`.
   b. Click **Change** next to the **Password** field.

      The **New Password** window opens.
   c. Use the window options to set a password.
3. Make sure **Enable data collection for ePO** is selected.
4. Click **Save Changes.**

6 Settings

Settings are used on the appliance for configuring modules, actions, and system functions.

Accordingly, you work with these settings in different ways.

Settings appear in different places on the user interface, for example, in the criteria, action, and events of rules or on the Settings and Appliances tabs.

At the initial setup of the appliance, settings are implemented together with the rule set system.

You can then review the settings of the implemented system, modify and delete them, and also create your own lists.

Contents

Types of settings

Different types of settings are used in rule processing and with other functions on the appliance.

- **Module settings** — Settings for the modules (also known as *engines*) that are called by rules to deliver values for properties and perform other jobs
- **Action settings** — Settings for the actions that rules execute
- **System settings** — Settings of the appliance system

Module settings

Module settings are settings for the modules (also knowns as *engines*) that are called by rules to deliver values for properties and perform other jobs.

For example, the URL Filter module retrieves information on URL categories to deliver values for the URL.Categories property in a filtering rule.

In a rule, the settings name for a module that is called by the rule appears next to a rule property. For example, in a rule for virus and malware filtering, *Gateway Antimalware*can appear as the settings name next to the *Antimalware.Infected* property.

This means that when the Anti-Malware module is called to deliver the value *true* or *false* for the property, the module runs with the *Gateway Antimalware* settings. These settings specify, for example, which methods are used in scanning web objects for infections.

You can access module settings in rules and on the lower main branch of the settings tree on the Settings tab.

You can modify these settings and also create new settings.

Action settings

Action settings are settings for the actions that are executed by rules.

They are mainly configured to specify the messages that are sent to users who are affected by rule actions, such as Block or Authenticate. Actions that do not affect users have no settings, for example, Continue or Stop Rule Set.

You can access these settings in rules and on the upper main branch of the settings tree on the Settings tab.

You can modify these settings and also create new settings.

System settings

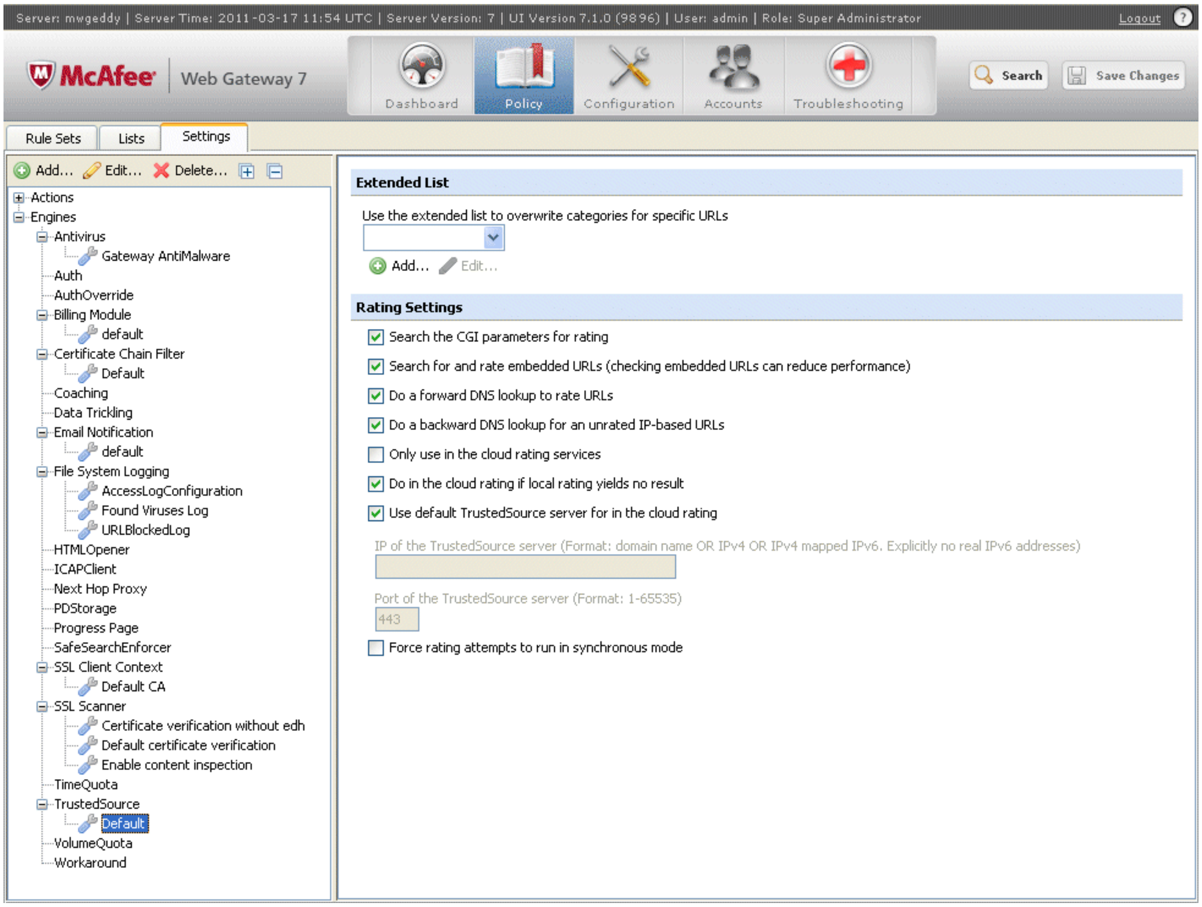
System settings are settings of the appliance system, for example, network interface settings or domain name system settings

You can access these settings on the **Appliances** tab of the **Configuration** top-level menu.

You can modify these settings, but not create new system settings.

Settings tab

The **Settings** tab allows you to work with settings for actions and modules.



Extended List

Use the extended list to overwrite categories for specific URLs

Rating Settings

☑ Search the CGI parameters for rating

☑ Search for and rate embedded URLs (checking embedded URLs can reduce performance)

☑ Do a forward DNS lookup to rate URLs

☑ Do a backward DNS lookup for an unrated IP-based URLs

☐ Only use in the cloud rating services

☑ Do in the cloud rating if local rating yields no result

☑ Use default TrustedSource server for in the cloud rating

IP of the TrustedSource server (Format: domain name OR IPv4 OR IPv4 mapped IPv6. Explicitly no real IPv6 addresses)

Port of the TrustedSource server (Format: 1-65535)
443

☐ Force rating attempts to run in synchronous mode

Main elements of the Settings tab

The following table describes the main elements of the **Settings** tab.

Table 6-1 Main elements of the Settings tab

Element	Description
Settings toolbar	Controls for working with settings for actions and modules (engines)
Settings tree	Tree structure displaying actions and modules (engines)
Settings	Parameters and values of the currently selected action or module (engine)

Settings toolbar

The settings toolbar provides the following options.

Table 6-2 Settings toolbar

Option	Definition
Add	Opens the **Add Settings** window for creating new settings.
Edit	Opens the **Edit Settings** window for editing existing settings.
Delete	Deletes the selected settings. A window opens to let you confirm the deletion.
Expand all	Expands all collapsed items on the settings tree.
Collapse all	Lets all expanded items on the settings tree collapse.

Access settings

You can access settings on the **Settings** tab or by clicking a settings name in a rule. For accessing system settings, you must work with the **Appliance** tab of the **Configuration** top-level menu.

Tasks

- *Access action and module settings on the Settings tab* on page 95
  You can use the **Settings** tab to access settings for actions and modules.
- *Access action and module settings in a rule* on page 96
  You can click names of settings for actions and modules that appear in rules to access these settings.
- *Access system settings* on page 96
  You can access system settings using the **Configuration** top-level menu.

Access action and module settings on the Settings tab

You can use the **Settings** tab to access settings for actions and modules.

Task

1. Select **Policy** | **Settings**.

2. On the settings tree, navigate to the **Actions** or **Engines** branch to access the settings you want to work with.

3 To select settings, do one of the following:

- On the **Actions** branch, click an action to expand it, and select the action settings you want to access.
- On the **Engine** branch, click a module (also known as *engine)* to expand it, and select the module settings you want to access.

The parameters and values of the settings appear on the settings pane.

You can now work with the settings.

Access action and module settings in a rule

You can click names of settings for actions and modules that appear in rules to access these settings.

Task

1 Select **Policy** | **Rule Sets**

2 On the rule sets tree, select the rule set that contains the rule with the settings you want to access.

The rules of the rule set appear on the settings pane.

3 Make sure **Show details** is selected.

4 In the rule with the settings you want to access, click the settings name:

- In the rule criteria to access module settings
- In the rule action to access action settings

The **Edit Settings** window opens with the settings that you selected.

You can now work with the settings.

Access system settings

You can access system settings using the **Configuration** top-level menu.

Task

1 Select **Configuration** | **Appliances**

2 On the appliances tree, select the appliance you want to configure system settings for and click the settings name.

The parameters and values of the settings appear on the settings pane.

You can now work with the settings.

Create action and module settings

You can create settings for modules and actions.

When creating these settings, you do not create them completely new, but use existing settings that you give a new name and modify as needed.

Task

1 Select **Policy** | **Settings**.

2 To select the settings that should serve you as the starting point for creating new settings, use one of the following two methods:

- On the settings tree, select these settings and click **Add**.

  The **Add Settings** window opens with the parameters and values of the selected settings.

- Click **Add** right away.

  The **Add Settings** window opens.

  Select settings from the **Settings for** pane of the window.

  The parameters and values of these settings appear in the window.

3 In the **Name** field of the window, type a name for the new settings.

4 [Optional] In the **Comment** field, type a plain-text comment on the settings.

5 Modify the existing values of the settings as needed.

6 [Optional] Click the **Permissions** tab and configure who is allowed to access the settings.

7 Click **OK**.

The window closes and the new settings appear on the settings tree.

8 Click **Save Changes**.

7 Proxies

The appliance uses its proxy functions to intercept web traffic and transmit it if this is allowed by the filtering rules. You can configure these functions to meet the requirements of your network.

The following are key settings for proxies:

- **Network mode** — Explicit proxy mode or a transparent mode

  Specific settings can be configured for each of these modes.

- **Network protocol** — HTTP, HTTPS, FTP, ICAP, and instant messaging protocols

  Protocol settings are common proxy settings that can be configured for each of the network modes.

You can configure other common proxy settings and also implement special proxy solutions, for example, reverse HTTPS proxy or proxy auto-configuration.

Contents

Configure proxies

You can configure the proxy functions of the appliance as is appropriate for your network.

Complete the following high-level steps.

Task

1. Review the proxy settings.

   The following key settings are configured by default:

   - Network mode: Explicit proxy
   - Network protocol: HTTP

2. Modify these settings as needed.

You can, for example, do the following:

- Configure a different network mode.

  You can choose one of the following:

  - Explicit proxy mode with High Availability functions
  - Transparent router mode
  - Transparent bridge mode

  When running McAfee Web Gateway on a virtual machine, the transparent modes are not available.

- Configure a different network protocol.

  You can add one or more of the following to HTTP (or add them and disable HTTP):

  - HTTPS
  - FTP
  - ICAP
  - Instant messaging protocols: Yahoo, ICQ, Windows Live Messenger, XMPP (for Jabber and other services)

- Modify other proxy settings, for example, timeouts or the maximum number of client connections.

3 Configure a special proxy solution if needed, for example, reverse HTTPS proxy or proxy auto-configuration.

4 Save your changes.

Explicit proxy mode

In explicit proxy mode, the clients that have their web traffic filtered on the appliance “know” they are connected to it. They must explicitly be configured to direct their web traffic to the appliance.

If this is ensured, it is less important where the appliance is deployed within your network. Typically, it is placed behind a firewall and connected to its clients and the firewall by a router.

The following diagram shows a configuration in explicit proxy mode.

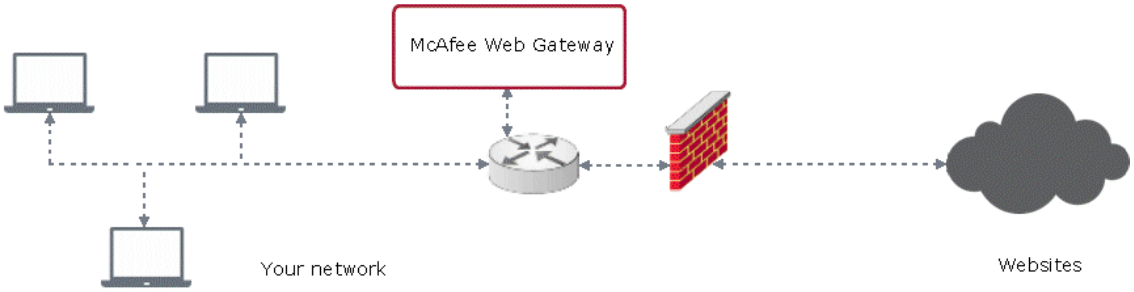


Figure 7-1 Explicit proxy mode

Configure the explicit proxy mode

You can configure the proxy functions of an appliance in explicit proxy mode, which is the default mode for these functions.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to configure the explicit proxy mode for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.
3. Under **Network Setup**, select one of the two options for the explicit proxy mode.
   - **Proxy** — For the explicit proxy mode

     ℹ This is the default proxy mode.

     When it is selected, specific settings for configuring transparent features of the explicit proxy mode appear below the **Network Setup** settings.
   - **Proxy HA** — For an explicit proxy mode with High Availability functions

     After selecting this option, specific **Proxy HA** settings appear below the **Network Setup** settings.
4. Configure specific and common settings for the selected option as needed.
5. Click **Save Changes**.

See also

Transparent Proxy settings on page 101
Proxy HA settings on page 105
Proxies settings on page 118

Transparent Proxy settings

The Transparent Proxy settings are used for configuring transparent features of the explicit proxy mode.

Transparent Proxy

Settings for configuring the explicit proxy mode with transparent features

Table 7-1 Transparent Proxy

Option	Definition
Supported client redirection methods	Methods for intercepting web traffic and directing it to the appliance • **WCCP** — When selected, client requests sent to web servers under the IPv4 protocol are intercepted by an additional network device and directed to the appliance using the WCCP protocol. In the same way responses from web servers are directed back to the appliance. The clients are not aware of this redirection, it remains transparent for them. Version 2 of WCCP must be used on the appliance. To use the WCCP redirection method, you need to configure one or more WCCP services on the appliance. You also need to configure the network device that intercepts the client requests and server responses. This device can be configured as a switch or router. After selecting this option, the **WCCP Services** inline list appears for configuring and adding WCCP services • **L2 transparent** — When selected, client requests sent to a web server under the IPv4 and IPv6 protocols are intercepted by an additional network device and directed to the appliance using the Layer 2 redirection method. Under this method, client requests are accepted on the appliance even if their destination IP addresses are not addresses of the appliance. The redirection is transparent to the clients. You need to enter the original ports for those client requests that are to be intercepted and redirected in a list on the appliance together with the ports that these requests are redirected to. The additional network device must be configured accordingly. When this option is selected, requests can not be transmitted using a connection in active FTP mode. Only the passive FTP mode is then available. After selecting this option, the **Port Redirects** inline list is displayed for entering ports.

The following two tables describe list entries in the lists of WCCP services and port redirects.

Table 7-2 WCCP Services – List entry

Option	Definition
Service ID	ID of a service that directs web traffic to the appliance under the WCCP protocol
WCCP router definition	Multicast IP address and DNS name of a router (or switch with routing functions) that uses a WCCP service to direct web traffic to the appliance You can configure multiple routers here, separating entries by commas.
Ports to be redirected	Ports on web servers that data packets must have in their destination addresses to be redirected You can specify up to eight port numbers here, separated by commas.
Ports to be redirected are source ports	Displays whether the ports that are to be redirected are source ports.
Proxy listener IP address	IP address of the appliance when running in explicit proxy mode with WCCP services and listening to client requests
Proxy listener port	Port for listening to client requests The default port number is 9090.

Table 7-2 WCCP Services – List entry *(continued)*

Option	Definition
MD5 authentication key	Password used under the MD5 algorithm for signing and verifying control data packets The **Set** button opens a window for setting the password. The password can have up to eight characters.
Input for load distribution	*This main item does not appear in the list, but is visible in the Add and Edit windows. The following four elements are related to it, specifying what is used in a data packet as the criteria for load distribution* When running multiple appliances, load distribution can be configured for the proxies on them. Data packets can be distributed to these proxies based on the masking of source or destination IP addresses and port numbers or on a hash algorithm. • **Source IP** — When selected, load distribution relies on the masking of source IP addresses. • **Destination IP** — When selected, load distribution relies on the masking of destination IP addresses. • **Source port** — When selected, load distribution relies on the masking of source port numbers. • **Destination port** — When selected, load distribution relies on the masking of destination port numbers.
Assignment method	*This main item does not appear in the list, but is visible in the Add and Edit windows. The following two elements are related to it, specifying the assignment method.* • **Assignment by mask** — When selected, masking of the parameter specified above is used for load distribution. • **Assignment by hash** — When selected, a hash algorithm is used for load distribution.
Assignment weight	Value determining how much load is assigned to a proxy Use this value to assign more load to a proxy on an appliance that has more CPU capacity. 0 means no load is distributed to a proxy.
Forwarding method	*This main item does not appear in the list, but is visible in the Add and Edit windows. The following two elements are related to it, specifying the forwarding method.* • **GRE-encapsulated** — When selected, data packets are encapsulated by the router before being redirected. • **L2-rewrite to local NIC** — When selected, data packets are redirected to the appliance by replacing the MAC address of the next device (on the route to the web server) with that of the appliance.
L2-redirect target	Network interface on an appliance that data packets are redirected to
Magic (Mask assignment)	Unknown field in the mask that the appliance sends to the router This setting is needed for ensuring compatibility with different versions of the vendor's operating system, which is used for the router.
Comment	Plain-text comment on a WCCP service

Table 7-3 Port redirects – List entry

Option	Definition
Original destination port	Port that the data packets belonging to a client request were originally directed to
Destination proxy port	Port that data packets are redirected to
Comment	Plain-text comment on a port redirect

Advanced Outgoing Connections Settings

Settings specifying methods for handling information contained in client requests sent to web servers that are requirements for the network environment of the appliance

Table 7-4 Advanced Outgoing Connections Settings

Option	Definition
IP spoofing (HTTP, HTTPS, FTP)	When selected, the appliance keeps the client IP address that is contained in a client request as the source address and uses it in communication with the requested web server under various protocols. When WCCP services are used for intercepting web traffic and directing it to the appliance, you need to configure two services for each port on the appliance that listens to client requests: one for the requests that come in from the clients, and one for responses to these requests that are sent by the web servers. When this option is not selected, the appliance chooses a source port and uses it in this communication. • **IP spoofing for explicit proxy connections** — When selected, client addresses are kept in explicit proxy mode, in which web traffic is not intercepted by an additional device. • **Use same source port as client for IP spoofing** — When selected, client source ports are kept and used in addition to client source addresses for communication with web servers. When this option is not selected, the appliance chooses a random source port and uses it in this communication.
HTTP(S): Host header has priority over original destination address (transparent proxy)	When selected, the appliance uses the destination address that is included in the host header of a client request under the HTTP or HTTPS protocol for communication with the requested web server.

Sample WCCP service settings for IP spoofing

Sample settings for configuring WCCP services with IP spoofing

You can use IP spoofing in a configuration with WCCP services that intercept web traffic and direct it to the appliance. In this case, you need to configure two services for all ports on the appliance that listen.

One of these services is for the requests that come in from the clients and another one for responses to these requests that are sent by the web servers.

The following table shows sample parameter values for these two services.

Table 7-5 Sample parameter values for two WCCP services configured with IP spoofing

Option	Service for incoming requests	Service for web server responses
Service ID	51	52
WCCP router definition	10.150.107.254	10.150.107.254

Table 7-5 Sample parameter values for two WCCP services configured with IP spoofing *(continued)*

Option	Service for incoming requests	Service for web server responses
Ports to be redirected	80, 443	80, 443
Ports to be redirected are source ports	false	true
Proxy listener IP address	10.150.107.251	10.150.107.251
Proxy listener port	9090	9090
MD5 authentication key	* * * * *	* * * * *
Input for load distribution	*This main item does not appear in the settings list, but is visible in the Add and Edit windows. The following four elements are related to it*	
Source IP	false	false
Destination IP	true	true
Source port	false	false
Destination port	false	false
Assignment method	*This main item does not appear in the settings list, but is visible in the Add and Edit windows. The following four elements are related to it*	
Assignment by mask	true	true
Assignment by hash	false	false
Assignment weight	100	100
Forwarding method	*This main item does not appear in the settings list, but is visible in the Add and Edit windows. The GRE-encapsulated and L2-rewrite to local NIC elements are related to it*	
GRE-encapsulated	false	false
L2-rewrite to local NIC	true	true
L2-redirect target	eth1	eth1
Magic (Mask assignment)	-1	-1
Comment		

Proxy HA settings

The Proxy HA settings are used for configuring the proxy functions of the appliance in explicit proxy mode with High Availability functions.

Proxy HA

Settings for the explicit proxy mode with High Availability functions

Table 7-6 Proxy HA

Option	Definition
Port redirects	List of ports that requests sent by users are redirected to
Director priority	Priority (ranging from 0 to 99) an appliance takes in directing data packets The highest value prevails. 0 means the appliance never directs data packets, but only filters them. In a High Availability configuration, two appliances are typically configured as director nodes with a priority higher than zero to direct data packets, providing fail-over functions for each other. The remaining nodes are configured with zero priority (also known as *scanning nodes*). The priority value is set on a slider scale.
Management IP	Source IP address of the appliance that directs data packets when sending heartbeat messages to other appliances
Virtual IPs	List of virtual IP addresses

The following two tables describe entries in the list of port redirects and thet list of virtual IPs.

Table 7-7 Port redirects – List entry

Option	Definition
Protocol name	Name of the protocol used for data packets coming in when a user sends a request
Original destination ports	Ports that redirected data packets were originally sent to
Destination proxy port	Port that data packets sent to the above ports originally are redirected to
Comment	Plain-text comment on a port redirect

Table 7-8 Virtual IPs – List entry

Option	Definition
Virtual IP address	Virtual IP address (in CIDR notation)
Network interface	Network interface on the appliance used for heartbeats under VRRP (Virtual Router Redundancy Protocol)
Comment	Plain-text comment on a virtual IP address

Transparent router mode

The transparent router mode is one of the two transparent modes you can configure for the proxy functions of the appliance if you do not want to use an explicit mode.

In this mode, the clients are unware of the appliance and need not be configured to direct their web traffic to it.

The appliance is placed as a router immediately behind a firewall. It can use a switch for connecting to its clients. A routing table is used to direct the traffic.

The following diagram shows a configuration in transparent router mode.

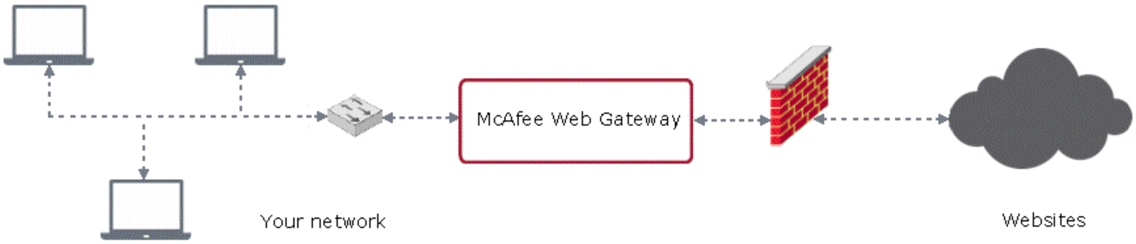


Figure 7-2 Transparent router mode

Configure the transparent router mode

You can configure the proxy functions of an appliance in transparent router mode.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to configure the transparent router mode for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3 Under **Network Setup**, select **Transparent Router**.

After selecting this mode, specific **Transparent Router** settings appear below the **Network Setup** settings.

4 Configure specific and common settings for this mode as needed.

5 Click **Save Changes**.

See also

Configure nodes in transparent router mode on page 107
Transparent Router settings on page 109
Proxies settings on page 118

Configure nodes in transparent router mode

You can configure two appliances that are nodes in a Central Management configuration as director and scanning nodes in transparent router mode. The director node directs data packets, while the scanning node filters them.

Tasks

- *Set up a director node in transparent router mode* on page 107
  To set up a director node in transparent router mode, you need to enable this mode and configure network interfaces for inbound and outbound web traffic.
- *Set up a scanning node in transparent router mode* on page 108
  To set up a scanning node in transparent router mode, you need to enable this mode and configure at least one network interface for outbound web traffic.

Set up a director node in transparent router mode

To set up a director node in transparent router mode, you need to enable this mode and configure network interfaces for inbound and outbound web traffic.

The director role is configured by giving the node an appropriate priority value.

Task

1 Select **Configuration | Appliance.**

2 On the appliances tree, select the appliance you want to set up as a director node and click **Network.**

3 Configure network interfaces as is suitable for your network.

You need at least one interface for inbound and one for outbound web traffic.

4 Click **Save Changes**

You are logged off and logged on to the appliance again.

5 Select **Configuration | Appliances.**

6 On the appliances tree, select the appliance you are setting up as a director node and click **Proxies (HTTP(S), FTP, ICAP, and IM).**

7 Under **Network Setup**, select **Transparent Router.**

After selecting this mode, specific **Transparent Router** settings appear below the **Network Setup** settings.

8 Set **Director priority** to a value > 0.

9 Configure proxy ports and port redirects for HTTP and FTP as needed.

10 Configure virtual IP addresses for the inbound and outbound network interfaces, using free IP addresses for this purpose.

11 In the **Management IP** field, type an IP address for reaching the scanning node.

12 Leave the number under **Virtual router ID** as it is.

13 From the **VRRP interface** list, select the interfaces for heartbeats under this protocol.

14 Configure IP spoofing as needed.

15 Click **Save Changes.**

Set up a scanning node in transparent router mode

To set up a scanning node in transparent router mode, you need to enable this mode and configure at least one network interface for outbound web traffic.

The scanning role is configured by assigning the node 0 as its priority value.

Task

1 Select **Configuration | Appliances.**

2 On the appliances tree, select the appliance you want to set up as a scanning node and click **Network.**

3 Configure network interfaces as is suitable for your network.

You need at least one interface for outbound web traffic.

4 Click **Save Changes**

You are logged off and logged on to the appliance again.

5 Select **Configuration | Appliances.**

6 On the appliances tree, select the appliance you want to set up as a scanning node and click **(HTTP(S), FTP, ICAP, and IM)**.

7 Under **Network Setup**, select **Transparent Router**.

After selecting this mode, specific **Transparent Router** settings appear below the **Network Setup** settings.

8 Set **Director priority** to 0.

9 Configure the same HTTP and FTP proxy ports and port redirects as for the director node.

10 Configure also IP spoofing in the same way as for the director node.

11 Click **Save Changes**.

Transparent Router settings

The Transparent Router settings are used for configuring the proxy functions of an appliance in transparent router mode.

Transparent Router

Settings for configuring the transparent router mode

Table 7-9 Transparent Router

Option	Definition
Port redirects	List of ports that requests sent by users are redirected to
Director priority	Priority (ranging from 0 to 99) that an appliance takes in directing data packets Director priority becomes relevant when an appliance is one of several nodes in a Central Management configuration. Then the node with the highest value is the director node that directs data packets while the other nodes only filter them. If you specify 0 for a node, it can never be a director node. The value for the director priority is set on a slider scale.
Management IP	Source IP address of the appliance that directs data packets when sending heartbeat messages to other appliances
Virtual IPs	List of virtual IP addresses
Virtual router ID	ID of a virtual router
VRRP interface	Network interface on an appliance for sending and receiving heartbeat messages
IP spoofing (HTTP, HTTPS)	When selected, the appliance keeps the client IP address that is contained in a client request as the source address and uses it in communication with the requested web server under various protocols. The appliance does not verify whether this address matches the host name of the request.
IP spoofing (FTP)	When selected, the appliance communicates with a web server under the FTP protocol in the same way as under the HTTP or HTTPS protocol to perform IP spoofing. For active FTP, this option must be enabled.

The following two tables describe entries in the list of port redirects and the list of virtual IPs.

Table 7-10 Port redirects – List entry

Option	Definition
Protocol name	Name of the protocol used for data packets coming in when a user sends a request
Original destination ports	Ports that redirected data packets were originally sent to
Destination proxy port	Port that data packets sent to the above ports originally are redirected to
Comment	Plain-text comment on a port redirect

Table 7-11 Virtual IPs – List entry

Option	Definition
Virtual IP address	Virtual IP address (in CIDR notation)
Network interface	Network interface on an appliance that the virtual IP address configured here is assigned to However, this virtual IP address is only assigned to the interface if the current node takes the role of the active director
Comment	Plain-text comment on a virtual IP address

Transparent bridge mode

The transparent bridge mode is one of the transparent modes you can configure for the proxy functions of the appliance if you do not want to use an explicit mode.

In this mode, the clients are unaware of the appliance and need not be configured to direct their web traffic to it. The appliance is usually placed between a firewall and a router, where it serves as an (invisible) bridge.

The following diagram shows a configuration in transparent bridge mode.

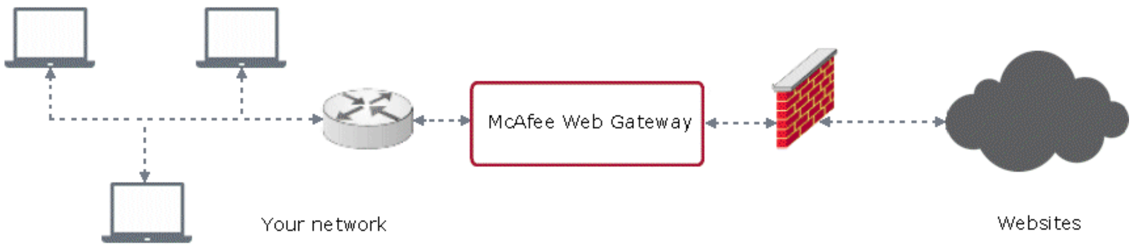


Figure 7-3 Transparent bridge mode

Configure the transparent bridge mode

You can configure the proxy functions of an appliance in transparent bridge mode.

Task

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to configure the transparent bridge mode for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3 Under **Network Setup**, select **Transparent Bridge**.

After selecting this mode, specific **Transparent Bridge** settings appear below the **Network Setup** settings.

4 Configure specific and common settings for this mode as needed.

5 Click **Save Changes**.

See also

Configure nodes in transparent bridge mode on page 111
Transparent Bridge settings on page 113
Proxies settings on page 118

Configure nodes in transparent bridge mode

You can configure two appliances that are nodes in a Central Management configuration as director and scanning nodes in transparent bridge mode. The director node directs data packets, while the scanning node filters them.

Tasks

- *Set up a director node in transparent bridge mode* on page 111
  To set up a director node in transparent bridge mode, you need to enable this mode and configure at least one network interface for the transparent bridge functions.
- *Set up a scanning node in transparent bridge mode* on page 112
  To set up a scanning node in transparent bridge mode, you need to enable this mode and configure an IP address that allows the node to access the network interface of the director node.

Set up a director node in transparent bridge mode

To set up a director node in transparent bridge mode, you need to enable this mode and configure at least one network interface for the transparent bridge functions.

The director role is configured by giving the node an appropriate priority value.

Task

1 Select **Configuration | Appliances**.

2 On the appliances tree, select the appliance you want to set up as a director node and click **Network**.

3 Select a still unused network interface of the appliance to use it as an interface of the transparent bridge, but do not enable it yet.

4 On the **Advanced** tab, select **Bridge enabled** for this interface.

5 In the **Name** field, type `ibr0` as the name of the interface.

6 On the **IPv4 tab**, under **IP Settings**, select **Disable IPv4**.

7 Click **Save Changes**.

You are logged off and logged on to the appliance again.

8 Select **Configuration | Appliances** and click **Network** again.

An additional network interface named **ibr0** is now available.

9 Select the **ibr0** interface.

10 On the **IPv4** tab, configure an IP address, a subnet mask, and a default route for **ibr0**.

11 Select the checkbox next to **ibr0** to enable this interface.

12 Select the interface that is currently used to access the appliance to assign it to **ibr0**.

13 On the **Advanced** tab, select **Bridge enabled**.

14 In the **Name** field, type `ibr0` as the name of the interface.

15 On the **IPv4** tab, under **IP Settings**, select **Disable IPv4**.

16 Enable the network interface you assigned to **ibr0** in step 3.

17 Select **Central Management**.

18 In the **Central Management Settings** section, add the IP address you configured for **ibr0** to the list provided under **IP address for Central Management communication**.

19 Select **Proxies (HTTP(S), FTP, ICAP, and IM)**.

20 Under **Network Setup**, select **Transparent Bridge**.

After selecting this mode, specific **Transparent Bridge** settings appear below the **Network Setup** settings.

21 Set **Director priority** to a value > 0.

22 Configure proxy ports and port redirects for HTTP and FTP as needed.

23 Configure also IP spoofing as needed.

24 In the **Management IP** field, type the IP address you configured for **ibr0**.

25 Click **Save Changes**.

Set up a scanning node in transparent bridge mode

To set up a scanning node in transparent bridge mode, you need to enable this mode and configure an IP address that allows the node to access the network interface of the director node.

The scanning role is configured by giving the node 0 as a priority value.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to set up as a scanning node and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3 Under **Network Setup**, select **Transparent Bridge**.

After selecting this mode, specific **Transparent Bridge** settings appear below the **Network Setup** settings.

4 Set **Director priority** to 0.

5 Configure the same HTTP and FTP proxy ports and port redirects as for the director node.

6 Configure also IP spoofing in the same way as for the director node.

7 Click **Save Changes**.

Transparent Bridge settings

The Transparent Bridge settings are used for configuring the proxy functions of an appliance in transparent bridge mode.

Transparent Bridge

Settings for configuring the transparent bridge mode

Table 7-12 Transparent Bridge

Option	Definition
Port redirects	List of ports that requests sent by users are redirected to
Director priority	Priority (ranging from 0 to 99) an appliance takes in directing data packets The highest value prevails. 0 means an appliance is what is known as a scanning node, which never directs data packets, but only filters them. The value for this priority is set on a slider scale. You can use this option only to configure a node as a scanning node (priority = 0) or a director node (priority > 0). Differences in node priorities greater than 0 are not evaluated. After configuring node priorities greater than 0 for multiple appliances in transparent bridge mode, you need to watch their behavior to find out which one has actually become the director node that directs data packets.
Management IP	Source IP address of the appliance that directs data packets when sending heartbeat messages to other appliances
IP spoofing (HTTP, HTTPS)	When selected, the appliance keeps the client IP address that is contained in a client request as the source address and uses it in communication with the requested web server under various protocols. The appliance does not verify whether this address matches the host name of the request.
IP spoofing (FTP)	When selected, the appliance communicates with a web server under the FTP protocol in the same way as under the HTTP or HTTPS protocol to perform IP spoofing For active FTP, this option must be enabled.

The following table describes an entry in the list of port redirects.

Table 7-13 Port redirects – List entry

Option	Definition
Protocol name	Name of the protocol used for data packets coming in when a user sends a request
Original destination ports	Ports that redirected data packets were originally sent to
Destination proxy port	Port that data packets sent to the above ports originally are redirected to
Comment	Plain-text comment on a port redirect

Instant messaging

Instant messaging proxies can be set up on an appliance to filter instant messaging (IM) chat and file transfer.

When users of your network participate in instant messaging communication, they send, for example, chat messages to an instant messaging server, receive responses to their messages, or send and receive files. An instant messaging proxy on an appliance can intercept and filter this traffic according to the implemented filtering rules. For this purpose, instant messaging traffic is redirected to the appliance.

The following network components are involved in the filtering process:

- **Instant messaging proxies** — Proxies can be set up on an appliance to filter instant messaging under different protocols, for example, a Yahoo proxy, a Windows Live Messenger proxy, and others.
- **Instant messaging clients** — These clients run on the systems of the users within your network to enable communication with instant messaging servers.
- **Instant messaging servers** — These are the destinations that are addressed by client from within your network.
- **Other components of your network** — Other components involved in instant messaging filtering can be, for example, a firewall or a local DNS server that redirects instant messaging traffic to an appliance.

When configuring instant messaging filtering, you need to complete configuration activities for the instant messaging proxy or proxies to ensure they intercept and filter the instant messaging traffic.

You also need to ensure that the instant messaging traffic is redirected to the instant messaging proxies. However, configuration activities for this are not performed on the clients, but on other components of your network. For example, DNS redirects or firewall rules are configured in a suitable manner.

An instant messaging proxy on an appliance is mainly intended to be used together with vendor IM client software that is provided, for example, by Yahoo, Microsoft, ICQ, or Google. But this client software can still change its behavior, for example, use a new logon server, without advance warning after a hidden update.

When using third-party client software, you should generally be aware that logon servers, protocol versions, or authentication methods could have been modified in comparison to those of the original client software, which can prevent an instant messaging proxy on an appliance from intercepting and filtering instant messaging traffic.

Configuring an instant messaging proxy

To configure an instant messaging proxy on an appliance, you need to configure the relevant parts of the **Proxies** settings of the **Configuration** top-level menu.

These are mainly settings for:

- Enabling an instant messaging proxy
- IP address and ports for listening to requests sent by instant messaging clients
- Settings for instant messaging servers
- Timeouts for instant messaging communication

Default values are preconfigured for all these settings after the initial setup of an appliance.

Instant messaging going on under the following protocols can be filtered:

- Yahoo
- ICQ
- Windows Live Messenger
- XMPP, which is the protocol used for Google Talk, Facebook Chat, Jabber, and other instant messaging services

The rules that are processed on an appliance for filtering instant messaging traffic are those that have *Requests (and IM)* configured as the processing cycle in the settings of their rule sets.

However, the *Responses* cycle can also be involved when instant messaging under the Yahoo protocol is filtered. Under this protocol, a requested file is transferred to a client in a response of the same kind as a response used for transferring files in normal web traffic. The file is stored on a server and retrieved by the client under HTTP, for example, using a suitable URL.

When problems arise in the communication between instant messaging client and proxy under a particular protocol, the client can also switch to using a different protocol and bypass the proxy this way. The client can even use a protocol for normal web traffic. On the dashboard of an appliance, this would result in a decrease of the IM traffic and an increase of the web traffic that is displayed.

Session initialization

During initialization of an instant messaging session between client and server, client requests can only be received on an appliance, but no responses can be sent back. As long as this is the case, the *IM.Message.CanSendBack* property will have *false* as its value when used in a rule.

We recommend that you do not implement any blocking rules with regard to session initialization, unless you want to block instant messaging traffic completely. You should also allow required helper connections, which are typically DNS requests or HTTP transfers.

Restrictions that you implement, for example, allowing only authenticated users, should rather apply to traffic going on during the session itself, such as chat messages and file transfers.

Configuring other network components for instant messaging filtering

The purpose of configuring other network components for instant messaging filtering is to redirect the instant messaging traffic that is going on between clients and servers to an appliance that has one or more instant messaging proxies running.

For example, under the ICQ protocol, clients send their requests to a server with the host name *api.icq.net*. For instant messaging filtering, you need to create a DNS redirecting rule that lets this host name be resolved not to the IP address of the ICQ server, but to that of the appliance.

In a similar way, firewall rules can be created to direct instant messaging traffic to an appliance rather than to an instant messaging server.

Filtering instant messaging traffic under Windows Live Messenger

When configuring the filtering of instant messaging traffic that is going on under the Windows Live Messenger protocol, the following is useful to know.

The host name of the instant messaging server is *messenger.hotmail.com*. This is the host name that must be resolved in a redirecting rule by the IP address of an appliance with an instant messaging proxy.

Sometimes a client connects to the server without requesting the host name to be resolved in a DNS lookup. In this case, it can help to find and remove the following registry entry within the client settings:

```
geohostingserver_messenger.hotmail.com:1863, REG_SZ
```

For a successful logon to a server, the following URL must be accessible to a client without authentication:

http://login.live.com

For this reason, you need to insert this URL in the whitelists that are used by the implemented web filtering rules on an appliance.

Filtering Instant messaging traffic under ICQ

When configuring the filtering of instant messaging traffic that is going on under the ICQ protocol, the following is useful to know.

The host names of the instant messaging servers are as follows:

- *api.icq.net* (Service request server: new since parting from AOL)
- *ars.icq.com* (File transfer proxy: new since parting from AOL)
- *api.oscar.aol.com* (Old service request server)
- *ars.oscar.aol.com* (Old file transfer proxy)
- *login.icq.com* (For old logon procedure)
- *login.oscar.aol.com* (For old logon procedure)

ICQ clients log on to a server in an encrypted process that cannot be intercepted by the instant messaging proxy on an appliance.

But after this, an ICQ client asks the service request server for information about the session server, using the magic token received after the logon. Here the instant messaging proxy intercepts. The filtering process then uses another logon procedure after the client name has been announced in the communication with the session server.

In contrast to the vendor Yahoo client, the vendor ICQ client ignores any Internet Explorer connection settings.

Filtering instant messaging traffic under Yahoo

When configuring the filtering of instant messaging traffic that is going on under the Yahoo protocol, the following is useful to know.

The list of instant messaging servers that requests are sent to can be very long. The following is a list of the host names of servers that are or have been in use. New servers can have appeared by now that would have to be added to the list.

- *vcs.msg.yahoo.com*
- *vcs1.msg.yahoo.com*
- *vcs2.msg.yahoo.com*
- *scs.yahoo.com*
- *cs.yahoo.com*
- *relay.msg.yahoo.com*
- *scs.msg.yahoo.com*
- *scs-fooa.msg.yahoo.com*
- *scs-foob.msg.yahoo.com*
- *scs-fooc.msg.yahoo.com*
- *scs-food.msg.yahoo.com*
- *scs-fooe.msg.yahoo.com*

- *relay1.msg.dcn.yahoo.com*
- *relay2.msg.dcn.yahoo.com*
- *relay3.msg.dcn.yahoo.com*
- *mcs.msg.yahoo.com*
- *scs.msg.yahoo.com*
- *scsa.msg.yahoo.com*
- *scsb.msg.yahoo.com*
- *scs-foof.msg.yahoo.com*
- *scsd.msg.yahoo.com*
- *scse.msg.yahoo.com*
- *scsf.msg.yahoo.com*
- *scsg.msg.yahoo.com*
- *scsh.msg.yahoo.com*

For a successful logon to a server, the following URLs must be accessible to a client without authentication:

- *http://vcs1.msg.yahoo.com/capacity*
- *http://vcs2.msg.yahoo.com/capacity*

For this reason, you need to insert these URLs in the whitelists that are used by the implemented web filtering rules on an appliance.

Even if the option **Connect directly to the Internet** has been enabled within the settings on a Yahoo client, it might still use Internet Explorer connection settings. This can cause the logon to fail in a later stage of the process. Therefore, we recommend that you also insert the URL **login.yahoo.com** in a whitelist.

Issues with instant messaging filtering

Issues with instant messaging filtering can involve, for example, the connection between client and server or the application of the implemented filtering rules.

Keep-alive data packets are sent in regular intervals as part of the instant messaging traffic to indicate the communication partners are still connected and responsive. Intervals vary between 20 and 80 seconds, depending on the IM protocol and client software. These data packets are not processed by the filtering rules that are implemented on an appliance.

If you detect such data packets in a troubleshooting situation, you can use rule engine tracing to see which rules are still executed.

When a client sends a request for logon to the server, it is redirected to the appliance if you have configured the appropriate settings. However, a client can at the same time try to log on to another server that requires SSL-secured authentication. If this fails, the client can also drop the connection to the appliance.

Some clients also provide options for performing basic troubleshooting tests after a failure to log on to the server.

Configure common proxy settings

You can configure common proxy settings in addition to the specific settings for a network mode.

Task

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to configure common proxy settings for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3 Configure these settings as needed.

4 Click **Save Changes**.

See also
Proxies settings on page 118

Proxies settings

The Proxies settings are used for configuring specific and common functions of the network modes that can be implemented on an appliance.

Network Setup

Settings for implementing a network mode

When a network mode is selected, specific settings for this mode appear below these settings.

Table 7-14 Network Setup

Option	Definition
Proxy (optional WCCP)	When selected, the explicit proxy mode is used and WCCP services can redirect web traffic to an appliance.
Proxy HA	When selected, the explicit proxy mode with High Availability functions is used.
Transparent router	When selected, the transparent router mode is used.
Transparent bridge	When selected, the transparent bridge mode is used.

HTTP Proxy

Settings for running a proxy on an appliance under the HTTP protocol

This protocol is used for transferring web pages and other data (providing also SSL-encryption for enhanced security).

Table 7-15 HTTP Proxy

Option	Definition
Enable HTTP proxy	When selected, a proxy is run on an appliance under the HTTP protocol
HTTP Port Definition list	List of ports on an appliance that listen to client requests
Anonymous login for FTP over HTTP	User name for logging on as an anonymous user when requests are transmitted to an FTP server by an appliance running as an HTTP proxy
Password for anonymous login for FTP over HTTP	Password for the above user name

FTP Proxy

Settings for running a proxy on an appliance under the FTP protocol

This protocol is used for transferring files, using separate connections for control functions and data transfer.

Table 7-16 FTP Proxy

Option	Definition
Enable FTP proxy	When selected, a proxy is run on an appliance under the FTP protocol.
FTP Port Definition list	List of ports on the appliance that listen to client requests

ICAP Server

Settings for running an ICAP server on an appliance that modifies requests and responses in communication with ICAP clients

Table 7-17 ICAP Server

Option	Definition
Enable ICAP server	When selected, an ICAP server is run on an appliance.
ICAP Port Definition list	List of ports on an appliance that listen to requests from ICAP clients

Web Cache

Setting for enabling the web cache on an appliance

In addition to enabling the web cache, you need to implement a rule set to control reading from and writing to the cache.

Table 7-18 Web Cache

Option	Definition
Enable cache	When selected, the web cache is enabled on an appliance.

Timeouts for HTTP(S), FTP, and ICAP

Settings for timeouts on connections for communication under the HTTP, HTTPS, FTP, and ICAP protocols

Table 7-19 Timeouts for HTTP(S), FTP, and ICAP

Option	Definition
Initial connection timeout	Time (in seconds) to elapse before a newly opened connection is closed if no request is received
Connection timeout	Time (in seconds) to elapse before a connection is closed if a client or server remains inactive during an uncompleted request communication
Client connection timeout	Time (in seconds) to elapse before a connection from the proxy on the appliance to a client is closed between one request and the next
Maximum idle time for unused HTTP server connections	Time (in seconds) to elapse before a connection from the proxy on the appliance to a server is closed between one request and the next

DNS Settings

Settings for communication with a domain name system server

Table 7-20 DNS Settings

Option	Definition
IP protocol version preference	Information on the version of the IP protocol that is used for the communication • (Version options) • **Same as incoming connection** — When selected, the protocol version is used that is already in use on the incoming connection. • **IP4** — When selected, version 4 of the IP protocol is used. • **IP6** — When selected, version 6 of the IP protocol is used. • **Use other protocol version as fallback** — When selected, the other protocol version is used if one of the two versions is not available.
Minimal TTL for DNS cache	Minimum time (in seconds) to elapse before data stored in the cache is deleted
Maximal TTL for DNS cache	Maximum time (in seconds) to elapse before data stored in the cache is deleted

Yahoo

Settings for running an instant messaging proxy under the Yahoo protocol on an appliance

Table 7-21 Yahoo

Option	Definition
Enable Yahoo proxy	When selected, a proxy for instant messaging under the Yahoo protocol is run on an appliance.
Listener address	IP address of the proxy and number of the port for listening to client requests.
Support file transfer over 0.0.0.0:80	When selected, requests for file transfers can use this IP address and port.
Login server	Host name and port number of the server that users log on to before sending requests
Relay server (Japan)	Host name and port number of the server used as a relay station when transferring files
Yahoo client connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a client is closed
Yahoo server connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a server is closed

ICQ

Settings for running an instant messaging proxy under the OSCAR (Open System for Communication in Real Time) protocol on an appliance

Table 7-22 ICQ

Option	Definition
Enable ICQ proxy	When selected, a proxy for instant messaging under OSCAR is run on an appliance.
Login and file transfer proxy port	IP address of an appliance that an instant messaging proxy is run on and number of the port for handling logon and file transfer • **Enable additional file transfer proxy port** — When selected, an additional port can be used for handling file transfers. • **Additional file transfer proxy port** — Additional IP address and port number for handling file transfers
BOS listener port	IP address of an appliance that an instant messaging proxy is run on and number of the port for listening to BOS (Basic OSCAR Service) requests, which include chat messages, as opposed to, for example, file transfers
ICQ login server	Host name and port number of the server that users log on to before sending requests
ICQ service request server	Host name and port number of the server that handles requests
ICQ file transfer proxy	Host name and port number of the server that handles file transfers
ICQ client connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a client is closed
ICQ server connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a server is closed

Windows Live Messenger

Settings for running an instant messaging proxy under the Windows Live Messenger protocol on an appliance

Table 7-23 ICQ

Option	Definition
Enable Windows Live Messenger proxy	When selected, a proxy for instant messaging under Windows Live Messenger is run on an appliance
Windows Live Messenger NS proxy listener 1	IP address of an appliance that an instant messaging proxy is run on and number of the first port that listens to client requests
Windows Live Messenger NS proxy listener 2	IP address of an appliance that an instant messaging proxy is run on and number of the second port that listens to client requests
Windows Live Messenger SB proxy port	IP address of an appliance that an instant messaging proxy is run on and number of the port that listens to client requests sent in SB (Switchboard) mode
Windows Live Messenger client connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a client is closed
Windows Live Messenger server connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a server is closed

XMPP

Settings for running an instant messaging proxy under the XMPP protocol on an appliance

This is the protocol used for several instant messaging services including Jabber, Google Talk, Facebook Chat, and others.

Table 7-24 XMPP

Option	Definition
Enable XMPP proxy	When selected, a proxy for instant messaging under the XMPP protocol is run on an appliance
Proxy port	IP address of an appliance that an instant messaging proxy is run on and port number for the port that listens to requests sent under the XMPP protocol
Client connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a client is closed
Server connection timeout	Time (in seconds) to elapse before an inactive connection from the instant messaging proxy to a server is closed

Advanced Settings

Settings for advanced proxy functions

Table 7-25 Advanced Settings

Option	Definition
Maximal number of client connections	Maximum number of connections from a proxy on an appliance to its clients Specifying 0 means no maximum number is configured.
Number of working threads	Number of threads used for filtering and transmitting web objects when a proxy is run on an appliance
Number of threads for AV scanning	Number of threads used to scan web objects for infections by viruses and other malware when a proxy is run on an appliance
Use TCP no delay	When selected, delays on a proxy connection are avoided by not using the Nagle algorithm to assemble data packets. This algorithm enforces that packets are not sent before a certain amount of data has been collected.
Maximal TTL for DNS cache in seconds	Maximum time (in seconds) for storing host name information in the DNS cache
Timeout for errors for long running connections in minutes	Time (in minutes) to elapse before a long running connection that is inactive due to an error is closed
Check interval for long running connections	Time (in minutes) to elapse between check messages sent on long running connections
Internal path ID	ID of the path an appliance uses to forward internal requests (not requests received from clients), for example, requests for style sheets to display error messages
Bypass RESPmod for responses that must not contain a body	When selected, responses sent in communication under the ICAP protocol are not modified according to the RESPMOD mode if they do not include a body.
Call log handler for progress page updates and objects embedded in error templates	When selected, the rules in the log handler rule set that is implemented on the appliance are processed to deal with the specified updates and objects.
Allow connections to use local ports using proxy	When selected, local ports can be used for requests on an appliance that a proxy is run on.
Allow connections to use local ports using proxy	When selected, hop-by-hop headers are removed from requests received on an appliance that an HTTP or HTTPS proxy is run on.
HTTP(S): Remove all hop-by-hop headers	When selected, hop-by-hop headers are removed from requests received on an appliance that an HTTP or HTTPs proxy is run on.

Table 7-25 Advanced Settings *(continued)*

Option	Definition
HTTP(S): Inspect via headers to detect proxy loops	When selected, via headers in requests received on the appliance that an HTTP or HTTPS proxy is run on are inspected to detect loops.
HTTP(S): Host from absolute URL has priority over host header	When selected, the host names corresponding to absolute URLs in requests received on an appliance that an HTTP or HTTPS proxy is run on are preferred to the host names contained in the request headers.

Reverse HTTPS proxy

A reverse HTTPS proxy configuration can prevent clients from uploading unwanted data, such as malware or particular media types, to web servers under the HTTPS protocol.

In this configuration, HTTPS traffic is redirected to an appliance that a proxy is run on. It is inspected and eventually forwarded or blocked, according to the rules implemented on the appliance.

You can configure this in the following ways:

- Set up a transparent bridge or router
- Set up a DNS configuration that points directly to the appliance when access to a particular web server is requested

Redirection to an appliance can also be achieved by configuring proxy-aware connections that rely on the use of CONNECT headers.

However, this method would require an additional network device to assemble these headers for incoming requests. It is therefore not recommended.

In addition to configuring your network, you need to configure the handling of SSL certificates.

Optionally, you can configure additional settings that are not SSL-related to ensure a smooth operation of the reverse HTTPS proxy.

Redirect HTTPS traffic in transparent bridge or router mode

In transparent bridge or router mode, you can use a port redirect rule (also known as port forwarding rule) to direct HTTPS traffic to the proxy port on an appliance.

You also need to ensure that the redirected requests are treated as SSL-secured communication.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to redirect traffic to and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3 In the **Network Setup** section, select **Transparent bridge** (or **Transparent router**).

The section with the specific transparent bridge (or router) settings appears.

4 Under **Port redirects**, click **Add**.

The **Add Port Redirects** window opens.

5 Configure the following settings for a new port redirect rule:

- **Protocol name** — HTTP

  ℹ This setting covers connections under both the HTTP and HTTPS protocols.

- **Original destination ports** — 443

  If the web servers that are the destinations for requests can be reached under the HTTP protocol as well, you can add port 80 here (separated by a comma). This type of traffic is then also directed to the appliance.

- **Destination proxy port** — 9090

  This is the default proxy port on an appliance.

6 Click **OK**.

The window closes and the new rule appears on the list.

7 Under **HTTP proxy port**, make sure **Enable HTTP proxy** is selected and click **Add**.

The **Add HTTP Proxy Port** window opens.

8 Make sure the following is configured:

- **Serve transparent SSL connections** — Selected
- **Ports treated as SSL** — 443

9 Leave the other settings at their default values and click **OK**.

The window closes and the new HTTP proxy port appears on the list.

10 Click **Save Changes**.

Let the appliance listen to requests redirected by DNS entries

When requests under the HTTPS protocol are redirected to an appliance according to DNS entries, you can configure the proxy on the appliance to listen directly on the appropriate port. You also need to ensure that only SSL-secured connections are served.

Before you begin

If you want to configure the proxy in this way, make sure of the following:

- The host names of the requested web servers are not resolved to the appliance when the appliance does a DNS lookup.

  You can achieve this by entering the IP adresses of the web servers into the /etc/hosts file on the appliance or by using an appropriately configured internal DNS server.

- A rule set that handles content inspection is implemented on the appliance and enabled.

  A suitable rule set is provided in the default rule set system as nested rule set of the SSL Scanner rule set.

When using DNS entries, a port redirect rule cannot be applied because the purpose of such a rule is forwarding requests for other destinations to the appliance. However, due to the DNS entries, the appliance is already the destination.

You also need to ensure that only SSL-secured connections are served.

Task

1 Select **Configuration | Appliances**.

2 On the appliances tree, select the appliance that should listen to requests and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3 Under **HTTP proxy port**, make sure **Enable HTTP proxy** is selected and click **Add**.

   The **Add HTTP Proxy Port** window opens.

4 Configure the following settings for a new HTTP proxy port:

   - **Listener address** — 0.0.0.0:443

     This setting lets the appliance listen to requests for any web servers, regardless of their IP addresses. You can also specify a particular IP address here and restrict the appliance to listening for requests to the server in question.

     If you are running several network interface cards on your appliance, you can specify IP addresses (separated by commas) for as many web servers as there are network interface cards.

   - **Serve transparent SSL connections** — Selected

   - **Ports treated as SSL** — *

5 Leave the other settings at their default values and click **OK**.

   The window closes and the new proxy port appears on the list.

   If a web server should also be accessible under the HTTPS protocol, you need to add another HTTP proxy port with listener address 0.0.0.0:80 or the address of a particular web server.

6 Click **Save Changes**.

SSL certificates in a reverse HTTPS proxy configuration

A reverse HTTPS proxy configuration is usually set up to protect a limited number of web servers against the upload of unwanted data by clients. You need to import SSL certificates for these servers and add them to the appliance configuration.

In a reverse HTTPS proxy configuration, the appliance communicates in SSL-secured mode with its clients. The SSL certificates that the appliance sends to the clients during the SSL handshake cannot be issued, however, by its SSL Scanner module. Therefore, the appliance uses the original certificates of the web servers that the clients request access to.

You can import these certificates when configuring the settings for the SSL Client Context without CA module.

The appliance uses several methods to find the appropriate certificates for sending to its clients.

Choosing certificates for sending to the clients

To find out which certificate should be sent to a client in a given situation, the appliance scans the list of imported certificates. On this list, certificates are mapped to the host names of the web servers they belong to. The appliance then sends the certificate that is mapped to the name of the host that a client requested access to.

In an explicit proxy setup, the host name would be transmitted and made known to the appliance in the header of the CONNECT request.

In a transparent setup, the appliance uses the following methods to detect the host names:

- If a client sends an SNI extension, the host name can be found in a way that is similar to detecting it in an explicit proxy configuration.
- If client requests are redirected to the appliance according to DNS entries, the host name is known by the IP address that you specified when configuring redirection.

  In this case, you also need to create a rule set with rules that set the URL.Host property to the appropriate value for every IP address the appliance has been configured to listen to. This is to let the appliance know where to forward a request to when it has been filtered and allowed.
- If the transparent setup does not use redirection by DNS entries, the appliance will send a handshake message to the web server that a client requested, extract the common name from the certificate it receives from the web server, and use this common name to detect the appropriate host name.

  This method requires that the appliance and the web server communicate in SSL-secured mode, too. You can configure a setting on the appliance to ensure this mode is used.

Create settings for SSL certificates in a reverse HTTPS proxy configuration

You can create settings for the SSL certificates that are used for web servers in a reverse HTTPS proxy configuration and import the certificates when configuring these settings.

Task

1. Select **Policies** | **Settings**.
2. On the settings tree, select **Enable SSL Client Context without CA**.
3. Click **Add** above the settings tree.

   The **Add Settings** window opens.
4. In the **Name** field, enter a name for the settings you want to add, for example, `Imported web server certificates`.
5. [Optional] In the **Comments** field, type a plain-text comment on the settings.
6. [Optional] Select the **Permissions** tab and configure who is allowed to access the settings.
7. In the **Define SSL Client Context (Without Certificate Authority)** section, configure the settings parameters.
   a. On the toolbar of the inline list **Select server certificate by host or IP**, click **Add**.

      The **Add Host to Certificate Mapping** window opens.
   b. Click **Import** and use the options of the **Import Server Certificate** window that opens to import an SSL certificate for a web server.
   c. Configure the other parameters in the **Add Host to Certificate Mapping** window as needed.
   d. Click **OK**.

      The window closes and a new entry for mapping an SSL certificate to the host name of a web server appears in the inline list.
   e. Repeat substeps a to d if you want to add more mapping entries to the inline list.

f Select or deselect **SSL-Scanner functionality applies only to client connection**, according to whether the connection to the web server should be SSL-secured or not.

If you choose to let this connection be unsecured, you need to create a rule that changes the network protocol from HTTPS to HTTP.

g Configure the other settings parameters for the SSL client context as needed.

h Click **OK**.

The **Add Settings** window closes and the new settings appear on the settings tree.

8 Click **OK**.

The window closes and the new settings appear on the settings tree.

9 Click **Save Changes**.

You can use these settings in the rule for setting the client context that is provided in the SSL Scanner rule set of the default rule set system.

Set the URL.Host property in a reverse HTTPS proxy configuration

When client requests are redirected to the appliance by DNS entries in a reverse HTTPS proxy configuration, you need to set the IP address of a web server as values of the URL.Host property to let the appliance know where to forward requests to.

After filtering a request has led to the result that it is allowed, the appliance uses the URL.Host property that was submitted with the request to forward it to the requested web server.

When requests are redirected according to DNS entries, web servers are known to the appliance by their IP addresses. If the URL.Host property has the IP address of a web server as its value, the appliance forwards the request to the appropriate destination.

Setting the value of a URL.Host property to an IP address can be done by a rule. You need to create such a rule for each web server that the appliance should forward requests to.

These rules can be contained in a rule set of their own.

Tasks

- *Create a rule set for setting the URL.Host property* on page 127
  You can create a rule set with rules that set the IP address of a web server as the value of the URL.Host property.
- *Create rules for setting the URL.Host property* on page 128
  You can create rules that set the IP address of a web server as the value of the URL.Host property.

Create a rule set for setting the URL.Host property

You can create a rule set with rules that set the IP address of a web server as the value of the URL.Host property.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, navigate to the position where you want to insert the rule set.

3 Above the tree, click **Add** and select **Rule Set**.

The **Add New Rule Set** window opens.

4 Under **Name**, enter a suitable name for the new rule set, for example, **Set value of URL.Host to IP address**.

5 Make sure **Enable** is selected.

6 Under **Applies to** select **Requests and IM**.

7 Under **Apply this rule set**, select **Always**.

8 [Optional] Under **Comment**, type a plain-text comment on the rule set.

9 [Optional] Click the **Permissions** tab and configure who is allowed to access the rule set.

10 Click **OK**.

The window closes and the new rule set appears on the rule sets tree.

Create rules for setting the URL.Host property

You can create rules that set the IP address of a web server as the value of the URL.Host property.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select the rule set you have created for the new rules, for example, **Set value of URL.Host to IP address**.

3 Click **Add Rule**.

The **Add Rule** window opens with the **Name** step selected.

4 In the **Name** field, type a name for a new rule, for example, `Set value of URL.Host to 10.141.101.51`.

5 Select **Rule Criteria**, then **If the following criteria is matched**, and click **Add**.

The **Add Criteria** window opens.

6 Configure the rule criteria as follows:

a From the list of properties in the left column, select **URL.Destination.IP**.

b From the list of operators in the middle column, select **equals**.

c In the operand field under **Compare with** in the right column, type an IP address.

7 Click **OK**.

The window closes and the new criteria appears under **Rule Criteria**.

8 Click **Action**, select **Continue**, and leave the default settings for this action.

9 Click **Events**, then **Add**, and from the drop-down menu that appears, select **Set Property Value**.

The **Add Set Property** window opens.

10 Set a property as follows:

a Under **Set this property**, select **URL.Host**.

b Under **To concatenation of these strings**, click **Add**.

The **Please Enter a String** window opens.

c. In the **Parameter value** field, type the host name of the web server that has the IP address you are using in this rule.

d. Click **OK**.

   The window closes and the host name appears in the **Add Set Property** window.

11. Click **OK**.

    The window closes and the event for setting the *URL.Host* property appears under **Events**.

12. Click **Finish**.

    The **Add Rule** window closes and the new rule appears within the rule set that you have created for the value-setting rules.

13. Repeat Steps 3 to 12 for every other value-setting rule you want to create.

14. Click **Save Changes**.

Complete optional activities for a reverse HTTPS proxy configuration

In addition to configuring the network setup and the SSL certificate handling, you can complete several other activities, which are optional, to ensure a smooth operation of the reverse HTTPS proxy.

- Deactivate proxy loop detection
- Restrict access to appliance ports
- Restrict access to web servers
- Address multiple web servers

Tasks

- *Deactivate proxy loop detection* on page 130
  An appliance can detect proxy loops by evaluating the Via header of a client request. We recommend that you deactivate this detection process in a reverse HTTPS proxy configuration.
- *Restrict access to appliance ports* on page 130
  In a reverse HTTPS proxy configuration, access should be restricted to the proxy ports of an appliance. You need to configure the user interface and file server settings accordingly.
- *Restrict access to web servers* on page 130
  A reverse HTTPS proxy configuration is usually implemented to protect a limited number of web servers against unwanted data uploads from clients. In this configuration, you should allow access to these servers only and block it for others.
- *Address multiple web servers* on page 133
  You can let an appliance forward consecutive requests to different web servers to achieve load balancing and ensure redundancy.

Deactivate proxy loop detection

An appliance can detect proxy loops by evaluating the Via header of a client request. We recommend that you deactivate this detection process in a reverse HTTPS proxy configuration.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to deactivate proxy loop detection for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.
3. In the **Advanced Settings** section, deselect **HTTP(S): Inspect Via header to detect proxy loops**.
4. Click **Save Changes**.

Restrict access to appliance ports

In a reverse HTTPS proxy configuration, access should be restricted to the proxy ports of an appliance. You need to configure the user interface and file server settings accordingly.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to restrict port access for and click **User Interface**.
3. Under **HTTP Connector Port**, enter the appliance proxy port (default: 9090).
4. Select **File Server**.
5. Under **HTTP Connector Port**, enter the appliance proxy port (default: 9090).
6. Click **Save Changes**.

Restrict access to web servers

A reverse HTTPS proxy configuration is usually implemented to protect a limited number of web servers against unwanted data uploads from clients. In this configuration, you should allow access to these servers only and block it for others.

After access to others servers has been requested and blocked, we also recommend that you let the appliance close these connections.

To restrict access:

- Create a list of the web servers you want to protect
- Create a rule set for a blocking rule
- Create a rule that blocks access to other web servers and closes connections to clients after blocking their requests

Tasks

- *Create a list of protected web servers* on page 131
  You can create a list the web servers that you want to protect in a reverse HTTPS proxy configuration.
- *Create a rule set for a blocking rule* on page 131
  You can create a rule set for the rule thats blocks access to web servers in a reverse HTTPS proxy configuration.
- *Create a rule to block access to web servers* on page 132
  You can create a rule for blocking access to web servers when these are not on the list of protected servers in a reverse HTTPS proxy configuration.

Create a list of protected web servers

You can create a list the web servers that you want to protect in a reverse HTTPS proxy configuration.

Task

1. Select **Policy** | **Lists**.
2. Above the lists tree, click **Add**.

   The **Add List** window opens.
3. Configure the following settings for the list:
   - **Name** — List name, for example, `Protected web servers`
   - [Optional] **Comment** — A plain-text comment on the new list
   - **Type** — Wildcard Expression
4. [Optional] Click the **Permissions** tab and configure who is allowed to access the list.
5. Click **OK**.

   The window closes and the new list appears on the lists tree under **Custom Lists** | **WildcardExpression**.
6. To fill the list with entries, click **Add** above the settings pane.

   The **Add Wildcard Expression** window opens.

   To add multiple entries at once, click **Add Multiple**.
7. Enter one or more wildcard expressions matching the URLs for the web servers you want to protect. Separate multiple entries by commas.
8. Click **OK**.

   The window closes and the new entries appear on the list.
9. Click **Save Changes**.

Create a rule set for a blocking rule

You can create a rule set for the rule thats blocks access to web servers in a reverse HTTPS proxy configuration.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, navigate to the position where you want to insert the rule set.

3. Above the tree, click **Add** and select **Rule Set**.

   The **Add New Rule Set** window opens.

4. Under **Name**, enter a name for the new rule set, for example, `Block web servers in a reverse HTTPS proxy configuration`.

5. Make sure **Enable** is selected.

6. Under **Applies to**, select **Requests and IM**.

7. Under **Apply this rule set**, select **If the following criteria is matched**. Then click **Add**.

   The **Add Criteria** window opens.

8. Configure the rule set criteria as follows:

   a. From the **Property** list, select **URL.Protocol**.

   b. From the **Operator** list, select **equals**.

   c. Under **Operand**, type `https`.

   d. [Optional] Under **Comment**, type a plain-text comment on the new rule set.

9. [Optional] Click the **Permissions** tab and configure who is allowed to access the rule set.

10. Click **OK**.

    The window closes and the new rule set appears on the rule sets tree.

Create a rule to block access to web servers

You can create a rule for blocking access to web servers when these are not on the list of protected servers in a reverse HTTPS proxy configuration.

Task

1. Select **Policy | Rule Sets**.

2. On the rule sets tree, select the rule set you have created for the blocking rule, for example, **Block web servers in a reverse HTTPS proxy configuration**.

3. Click **Add Rule**.

   The **Add Rule** window opens with the **Name** step selected.

4. In the **Name** field, type a name for the rule, for example, `Allow access only to protected web servers`.

5. Select **Rule Criteria**, then **If the following criteria is matched** and click **Add**.

   The **Add Criteria** window opens.

6. Configure the rule criteria as follows:

   a. From the list of properties in the left column, select **URL.Host**.

   b. From the list of operators in the middle column, select **matches in list**.

   c. From the list of operands in the right column, select the web server list you configured, for example, **Protected web servers**.

7 Click **OK**.

The window closes and the new criteria appears under **Rule Criteria**.

8 Click **Action**, select **Block** and leave the default settings for this action.

9 Click **Events**, then **Add** and from the drop-down menu that appears, select **Event**.

The **Add Event** window opens.

10 Configure an event as follows:

a From the **Event** list, select **Enable Workaround**.

b From the **Settings** list, select **Do not keep connection to client persistent**.

11 Click **OK**.

The window closes and the new event appears under **Events**.

12 Click **Finish**.

The **Add Rule** window closes and the rule appears within the new rule set that you have created.

13 Click **Save Changes**.

Address multiple web servers

You can let an appliance forward consecutive requests to different web servers to achieve load balancing and ensure redundancy.

To implement this, you need to:

- Import the Next Hop Proxy rule set from the rule set library
- Create a list of next-hop proxies
- Create next-hop proxy settings
- Create a rule that uses the list and the settings to trigger the Enable Next Hop proxy event when a web server from the list of protected servers is requested.

  The list also uses a list of protected servers. For this list, you can use the one that you created to restrict access to these servers.

Tasks

- *Create a list of next-hop proxies* on page 134
  You can create a list of the web servers that are addressed as next-hop proxies when a suitable rule triggers the Enable Next Hop Proxy event.
- *Create next-hop proxy settings* on page 134
  You can create next-hop proxy settings for the rule that triggers the Enable Next Hop Proxy event when a server from the list of protected web servers is requested.
- *Create a rule for the Enable Next Hop proxy event* on page 135
  You can create a rule that triggers the Enable Next Hop proxy event when a server from the list of protected web servers is requested.

Create a list of next-hop proxies

You can create a list of the web servers that are addressed as next-hop proxies when a suitable rule triggers the Enable Next Hop Proxy event.

Task

1 Select **Policy** | **Lists**.

2 Above the lists tree, click **Add**.

The **Add List** window opens.

3 Configure the following settings for the list:

- **Name** — List name, for example, `Protected web servers as next-hop proxies`
- [Optional] **Comment** — Plain-text comment on the new list
- **Type** — NextHopProxy

4 [Optional] Click the **Permissions** tab and configure who is allowed to access the list.

5 Click **OK**.

The window closes and the new list appears on the lists tree under **Custom Lists** | **NextHopProxy**.

6 To fill the list with entries, click **Add** above the settings pane.

The **Add Wildcard Expression** window opens.

To add multiple entries at once, click **Add Multiple**.

7 Enter one or more wildcard expressions matching URLs for the web servers you want to address. Separate multiple entries by commas.

8 Click **OK**.

The window closes and the new entries appear on the list.

9 Click **Save Changes**.

Create next-hop proxy settings

You can create next-hop proxy settings for the rule that triggers the Enable Next Hop Proxy event when a server from the list of protected web servers is requested.

Task

1 Select **Policy** | **Settings**.

2 On the settings tree, select **Enable Next Hop Proxy** and click **Add**.

The **Add Settings** window opens.

3 Configure the following settings parameters:

- **Name** — Settings name, for example, `Protected web servers`
- [Optional] **Comment** — A plain-text comment on the new settings

4 Under **Next Hop Proxy Servers** configure the following:

   a From the **List of next hop proxy servers**, select the next hop proxy list you created, for example, `Protected web servers as next hop proxies`.

   b Make sure **Round Robin** is selected.

   c Deselect **Proxy style requests**.

5 Click **OK**.

   The window closes and the new settings appear on the settings tree.

6 Click **Save Changes**.

Create a rule for the Enable Next Hop proxy event

You can create a rule that triggers the Enable Next Hop proxy event when a server from the list of protected web servers is requested.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select the **Next Hop Proxy** rule set.

   The rules of this rule set appear on the settings pane.

3 Click **Add Rule**.

   The **Add Rule** window opens with the **Name** step selected.

4 In the **Name** field, type a name for the rule, for example, `Address protected web servers as next-hop proxies`.

5 Select **Rule Criteria**, then **If the following criteria is matched**, and click **Add**.

   The **Add Criteria** window opens.

6 Configure the rule criteria as follows:

   a From the list of properties in the left column, select **URL.Host**.

   b From the list of operators in the middle column, select **does not match in list**.

   c From the list of operands in the right column, select the web server list you configured to restrict access to these servers, for example, **Protected web servers**.

7 Click **OK**.

   The window closes and the new criteria appears under **Rule Criteria**.

8 Click **Action**, and leave the default **Continue**.

9 Click **Events**, then **Add** and from the drop-down menu that appears, select **Event**.

   The **Add Event** window opens.

10 Configure an event as follows:

   a From the **Event** list, select **Enable Next Hop Proxy**.

   b From the **Settings** list, select the settings you configured for this rule, for example, **Protected web servers**.

11 Click **OK**.

The window closes and the new event appears under **Events**.

12 Click **Finish**.

The **Add Rule** window closes and the new rule appears within the Next Hop Proxy rule set.

13 Click **Save Changes**.

Proxy auto-configuration

One or more proxy auto-configuration (PAC) files can be made available on an appliance for web browsers on clients. The browsers can use them to find proxies for accessing particular web pages.

A proxy auto-configuration file usually has *.pac* as its file name extension. There can be several of them on an appliance, for example, a *proxy.pac* and a *webgateway.pac*.

Under the WPAD (Web Proxy Auto-Discovery) protocol, a proxy auto-configuration file must have *wpad.dat* as its file name. Therefore, it can exist on an appliance only once.

Make a .pac file available

You can make a .pac file available for proxy auto-configuration to a web browser on a client.

Task

1 Store the .pac file in the /opt/mwg/files folder on the appliance.

2 Start the browser and navigate to the network configuration settings.

3 In the **Connection** section, click **Settings**.

4 Select **Automatic proxy configuration URL**, then enter the path and file name for the .pac file.

For example, enter:

```
http://mwgappl.webwasher.com:4711/files/proxy.pac
```

If you want the clients to use a dedicated port for downloading the file, you must first configure this port.

If no dedicated port is used, clients are directed to the HTTP port for the user interface (the default port number is 4711).

5 Click **OK**.

Create a rule for downloading a wpad.dat file

To enable the download of a wpad.dat file by a web browser on a client, you need to configure a rule that forwards the download request to the appropriate port on an appliance.

Task

1 On the user interface of the appliance, select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to make the wpad.dat file available on and click **Port Forwarding**.

3 Under **Port Forwarding Rules**, click **Add**.

The **Add AppliancePortForwarding** window opens.

4 Configure settings for a port forwarding rule as follows:

- **Source Host** — 0.0.0.0
- **Target Port** — 80
- **Destination Host** — 127.0.0.1
- **Destination Port** — <File download port>

  As <File download port>, enter the HTTP port for the user interface of the appliance (default: 4711) or a dedicated port that you have configured.

5 Click **OK**.

The window closes and the rule appears in the list.

Configure auto-detection of a wpad host

You can let a web browser use auto-detection to find the appliance as the host where a wpad.dat file is stored.

Task

1 Start the web browser and go to the network configuration settings.

2 In the **Connection** section, click **Settings**.

3 Select **Auto-detect proxy settings for this network**.

4 Click **OK**.

Using the Helix proxy

The Helix proxy is a third-party proxy for handling real-time streaming data.

It is initially not accessed from the user interface of the appliance, but from a command line interface, which is, for example, provided on your administration system.

After accessing the Helix proxy, you can administer it on its own user interface.

Configure use of the Helix proxy

You can configure the use of the Helix proxy from a command line interface.

Task

1 On the command line interface, enter an activation command for the Helix proxy.

This command could, for example, look as follows:

```
service helix-proxy activate
```

You are asked to enter a user name and password for the initial administrator account.

2. Enter both.

   The Helix proxy is started.

   After the start, you can find configuration files for the proxy in the */opt/helix-proxy* folder on the appliance and modify them manually as needed.

3. Connect to the user interface of the Helix proxy with the following command:

   ```
   http://<IP address of the Helix proxy>:21774/admin/index.html
   ```

   The user interface appears and displays a logon window.

4. Enter the user name and password from Step 2.

   After a successful logon, the user interface of the Helix proxy becomes accessible.

5. Use this interface for further configuration of the Helix proxy as needed.

6. Configure your real-player application to use the appliance as a proxy.

   This can be done, for example, in the following way:

   a. Start the real player.

   b. On its user interface, go to the proxy settings.

   c. In the appropriate input field, for example, the **RTSP** (Real-Time Streaming Protocol) field, enter the IP address of the appliance with 554 as the port number.

Secure ICAP

When an appliance takes the roles of server and client under the ICAP protocol, communication can be performed in SSL-secured mode.

To use this mode, you need to import a server certificate for each ICAP port on the appliance that should receive SSL-secured requests from its clients. The clients are not required to submit certificates.

Requests that should be directed from the appliance in its role as an ICAP client to the ICAP server must include ICAPS as a specification in the server address to enable SSL-secured communication with that server.

The appliance does not send a client certificate to the ICAP server.

XMPP proxy

When filtering instant messaging communication on an appliance, one of the methods you can use is to set up a proxy under the XMPP (Extensible Messaging and Presence Protocol).

This protocol is also known under the name of Jabber. It is used, for example, to participate in Facebook chats or Google talk going on between an XMPP client and server.

You can configure settings for the XMPP proxy on the user interface under **Configuration** | **Proxies**.

When the SSL Scanner rule set is not enabled on an appliance, traffic going on between an XMPP client and this appliance is not encrypted, but filtered by all rules that are enabled on the appliance. If the client does not accept unencrypted traffic, the connection is closed.

When the SSL Scanner rule set is enabled, traffic is encrypted and inspected using SSL scanning to make it available for filtering by other rules on the appliance.

8 Authentication

Users can be “filtered” on an appliance, which means you can allow web access only for those who are able to authenticate.

Authentication is not implemented by default, but there are preconfigured authentication rule sets, which you can use.

The types of authentication that you can implement include:

- **Standard authentication** — You can configure authentication for users who send requests for web access under a standard protocol, such as HTTP, HTTPS, or FTP.

  When the authentication rule set of the default rule set system is enabled, user information is by default retrieved from an internal user database.

  You can change this setting and configure a different method, such as NTLM, LDAP, Kerberos, and others.

- **Instant messaging authentication** — You can configure authentication for users who send requests for web access under an instant messaging protocol, such as Yahoo, Windows Live Messenger, ICQ, and others.

You can also control administrator access to an appliance by setting up and maintaining administrator accounts and roles.

Contents

Authentication process

Authentication ensures that users of your network cannot access the web if they are not able to authenticate. The authentication process looks up user information, for example, in an internal database or on a web server and blocks or allows access accordingly.

The following elements are involved in this process:

- Authentication rules that control the process
- The Authentication module, which retrieves information about users from a database

Authentication rules

An authentication rule set is included in the default rule set system, but not enabled by default. It contains rules that ask an unauthenticated user to authenticate and block requests from users who do not belong to one of the user groups on a particular list.

The rule set contains also whitelisting rules that allow users who send a request to skip authentication, depending on the IP address that a request was sent from or the URL that is requested.

Additional rule sets for other types of authentication, for example, IM and cookie authentication, are available in the rule set library.

You can review the rules in these rule sets, modify or delete them, and also create your own rules.

Authentication module

The Authentication module (also known as *engine*) retrieves information about users from a database. The module is called by the rules that need to know whether a user who requests access to a web object is authenticated.

Different methods of retrieving this information can be used:

- **NTLM** — Uses a database on a Windows domain server
- **NTLM Agent** — Uses an external agent on a Windows-based system for applying the NTLM authentication method
- **User Database** — Uses an internal database on the appliance

  This method is used by default when the rule set of the default rule set system is enabled.

- **LDAP** — Uses a database on an LDAP server
- **Novell eDirectory** — Uses data from a directory on a server that takes the role of an LDAP server
- **RADIUS** — Uses a database on a RADIUS server
- **Kerberos** — Uses a database on a Kerberos server
- **Authentication Server** — Uses a database on another external server

You can configure settings for the Authentication module to specify the authentication method and other parameters of the authentication process.

Configure authentication

You can implement authentication and adapt it to the needs of your network.

Complete the following high-level steps.

Task

1. Enable the Authenticate and Authorize rule set of the default rule set system.
2. Review the nested Authenticate with User Database rule set .

   This rule set contains a single rule, which asks unauthenticated users to authenticate.

   The rule criteria includes settings for the Authentication module, which specify use of the User Database authentication method. This means information for authenticating users is retrieved from an internal database on the appliance.
3. Modify the default rule set as needed.

   You can, for example, do the following:

   - Modify the common parameters of the Authentication module
   - Modify the specific parameters for the User Database method
   - Implement a different authentication method, for example, NTLM or LDAP
   - Modify the specific parameters for the new authentication method
4. Consider importing a rule set from the library to implement authentication for a different type of communication, for example, instant messaging authentication.
5. Save your changes.

Configure the Authentication module

You can configure the Authentication module to modify the way user information is retrieved to authenticate users.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, select the rule set for authentication.

   In the default rule set system, this is the *Authenticate and Authorize* rule set.
3. Select a rule that controlls user authentication and click the settings that are specified in the rule criteria.

   In the rule set of the rule set system, this is, for example, the rule **Authenticate with User Database** in the nested **Authenticate with User Database** rule set and the settings name is **User Database**.

   The **Edit Settings** window opens. It provides the settings for the Authentication module.
4. Configure these settings as needed.
5. Click **OK** to close the window.
6. Click **Save Changes**.

See also

Authentication settings on page 142

Authentication settings

The Authentication settings are used for configuring the way the Authentication module looks up information on users to authenticate them.

Authentication Method

Settings for selecting an authentication method

Table 8-1 Select Scanning Engines

Option	Definition
Authentication method	List for selecting an authentication method You can select one of the following: • NTLM • NTLM-Agent • User Database • LDAP • Novell eDirectory • RADIUS • Kerberos • Authentication Server After selecting a method, settings that are specific to it appear below the common settings

Authentication Test

Settings for testing whether a user with given credentials would be authenticated

Table 8-2 Authentication Test

Option	Definition
User	User name that is tested
Password	Tested password
Authenticate User	Executes the test.
Test result	Displays the outcome of the test.

Common Authentication Parameters

Settings common to all authentication methods

Table 8-3 Common Authentication Parameters

Option	Definition
Proxy Realm	Location of the proxy that receives requests from users who are asked to authenticate
Authentication attempt timeout	Time (in seconds) to elapse before the authentication process terminates if not completed successfully
Use authentication cache	When selected, authentication information is stored in a cache. Authentication is then based on this stored information, rather than on information retrieved from an authentication server or the internal user database.
Authentication cache TTL	Time (in minutes) that authentication information is stored in the cache

Advanced Parameters

Setting for configuring advanced authentication

This setting is the same for all authentication methods. For this reason, it is described here after the common settings. On the user interface, it follows the specific settings for the authentication method that are currently displayed.

Table 8-4 Advanced Parameters

Option	Definition
Always evaluate property value	When selected, a new evaluation to assign a value to a property is performed each time a rule containing this property is processed. If a value has been stored for a property in the cache, it is not used. While it is normally recommended to let cache values be used to improve performance, there can be situations where the new evaluation of a property is required. In these situations, the same property is used more than once within the authentication rules and with the same settings of the Authentication module. A new evaluation ensures the most current value is assigned to the property each time.

NTLM Specific Parameters

Settings for the NTLM authentication method

Table 8-5 NTLM Specific Parameters

Option	Definition
Default NTLM domain	Name of the default Windows domain used for looking up authentication information This is one of the domains you have configured on the **Appliances** tab of the **Configuration** top-level menu.
Get global groups	When selected, information on global user groups is searched for on the Windows domain server.
Get local groups	When selected, information on local user groups is searched for on the Windows domain server.
Prefix group name with domain name (domain\group)	When selected, the name of the Windows domain appears before the name of the user group when authentication information on this group is sent from the domain server.
Enable basic authentication	When selected, the basic NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then sent in plain-text format (less secure) to the Windows domain server.
Enable integrated authentication	When selected, the integrated NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then encrypted before it is sent to the Windows domain server.
Enable NTLM cache	When selected, NTLM authentication information is stored in this cache. Authentication is then based on this stored information, rather on information retrieved from the Windows domain server.
NTLM cache TTL	Time (in seconds) that authentication information is stored in this cache
International text support	Set of characters used by default for a request sent from a client, for example, ISO-8859-1

NTLM Agent Specific Parameters

Settings for the NTLM Agent authentication method

Table 8-6 NTLM Agent Specific Parameters

Option	Definition
Use secure agent connection	When selected, the connection used for communicating with the NTML Agent is SSL-secured
Authentication connection timeout in seconds	Time (in seconds) to elapse before the connections to the NTLM-Agent is closed if no activities occur on it
Agent Definition	List of agents that are available for performing NTLM authentication
Default NTLM domain	Name of the default Windows domain used for looking up authentication information This is one of the domains you have configured on the **Appliances** tab of the **Configuration** top-level menu.
Get global groups	When selected, information on global user groups is searched for on the Windows domain server.
Get local groups	When selected, information on local user groups is searched for on the Windows domain server.
Prefix group name with domain name (domain\group)	When selected, the name of the Windows domain appears before the name of the user group when authentication information on this group is sent from the domain server.
Enable basic authentication	When selected, the basic NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then sent in plain-text format (less secure) to the Windows domain server.
Enable integrated authentication	When selected, the integrated NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then encrypted before it is sent to the Windows domain server.
Enable NTLM cache	When selected, NTLM authentication information is stored in this cache. Authentication is then based on this stored information, rather on information retrieved from the Windows domain server.
NTLM cache TTL	Time (in seconds) that authentication information is stored in this cache International text support — Set of characters used by default for a request sent from a client, for example, ISO-8859-1
International text support	Set of characters used by default for a request sent from a client, for example, ISO-8859-1

User Database Specific Parameters

Settings for the User Database authentication method

Table 8-7 User Database Specific Parameters

Option	Definition
Send domain and machine name to the client	When selected, the names of the appliance and the domain it has been assigned to are sent to the client that a user who is to be authenticated sent a request from.
Enable basic authentication	When selected, the basic NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then sent in plain-text format (less secure) to the Windows domain server.

Table 8-7 User Database Specific Parameters *(continued)*

Option	Definition
Enable integrated authentication	When selected, the integrated NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then encrypted before it is sent to the Windows domain server.
Enable NTLM cache	When selected, NTLM authentication information is stored in this cache. Authentication is then based on this stored information, rather on information retrieved from the Windows domain server.
NTLM cache TTL	Time (in seconds) that authentication information is stored in this cache
International text support	Set of characters used by default for a request sent from a client, for example, ISO-8859-1

LDAP Specific Parameters

Settings for the LDAP authentication method

Table 8-8 LDAP Specific Parameters

Option	Definition
LDAP server(s) to connect to	List of LDAP servers to retrieve authentication information from
List of certificate authorities	List of certificate authorities for providing certificates when a Secure LDAP (S-LDAP) connection is used for communication with the LDAP server
Credentials	User name of the appliance for logging on to the LDAP server
Password	Password for the user name The **Set** button opens a window for configuring a new password.
International text support	Set of characters used by default for a request sent from a client, for example, ISO-8859-1
Enable LDAP version 3	When selected, version 3 of the LDAP protocol is used.
Allow LDAP library to follow referrals	When selected, the lookup of user information can be redirected from the LDAP server to other servers.
Connection live check	Time (in minutes) to elapse between checks to see whether the connection to the LDAP server is still active
LDAP operation timeout	Time (in seconds) to elapse before the connection to the LDAP server is closed if no communication occurs
Base distinguished name to user objects	Distinguished name (DN) in the directory on the LDAP server where the lookup of user attributes should begin
Map user name to DN	When selected, the name of the user who asks for authentication must map to a DN (Distinguished Name). This name identifies the user in the directory on the LDAP server
Filter expression to locate a user object	Filtering term for restricting the lookup of user attributes To substitute the user name in the filtering term, u% is used as a variable.
Get user attributes	When selected, user attributes are looked up on the LDAP server to authenticate a user.
User attributes to retrieve	List of user attributes to retrieve from the LDAP server
Attributes concatenation string	String for separating user attributes found by the lookup, for example, / (slash)

Table 8-8 LDAP Specific Parameters *(continued)*

Option	Definition
Get groups attributes	When selected, user group attributes are also looked up on the LDAP server to authenticate a user.
Base distinguished name to group objects	Distinguished name (DN) in the directory on the LDAP server where the lookup of group attributes should begin
Filter expression to locate a group object	Filtering term for restricting the lookup of group attributes To substitute the user name in the filtering term, *u%* is used as a variable.
Group attributes to retrieve	List of group attributes to retrieve from the LDAP server

Novell eDirectory Specific Parameters

Settings for the Novell eDirectory authentication method

Table 8-9 Novell eDirectory Specific Parameters

Option	Definition
LDAP server(s) to connect to	List of the eDirectory servers that take the role of LDAP servers to provide authentication information
List of certificate authorities	List of certificate authorities for providing certificates when a Secure LDAP (S-LDAP) connection is used for communication with the LDAP server
Credentials	User name of the appliance for logging on to the LDAP server
Password	Password for the user name The **Set** button opens a window for configuring a new password.
International text support	Set of characters used by default for a request sent from a client, for example, ISO-8859-1
Enable LDAP version 3	When selected, version 3 of the LDAP protocol is used.
Allow LDAP library to follow referrals	When selected, the lookup of user information can be redirected from the LDAP server to other servers.
Connection live check	Time (in minutes) to elapse between checks to see whether the connection to the LDAP server is still active
LDAP operation timeout	Time (in seconds) to elapse before the connection to the LDAP server is closed if no communication occurs
eDirectory network address attribute	Name of the attribute that provides the network addresses used for the eDirectory server
eDirectory network login time attribute	Name of the attribute that provides the logon time used on the eDirectory server
eDirectory network minimal update interval	Time to elapse (in seconds) before information from the eDirectory server is updated
Base distinguished name to user objects	Distinguished name (DN) in the directory on the LDAP server where the lookup of user attributes should begin
Map user name to DN	When selected, the name of the user who asks for authentication must map to a DN (Distinguished Name). This name identifies the user in the directory on the LDAP server.
Filter expression to locate a user object	Filtering term for restricting the lookup of user attributes To substitute the user name in the filtering term, u% is used as a variable.
Get user attributes	When selected, user attributes are looked up on the LDAP server to authenticate a user.
User attributes to retrieve	List of user attributes to retrieve from the LDAP server

Table 8-9 Novell eDirectory Specific Parameters *(continued)*

Option	Definition
Attributes concatenation string	String for separating user attributes found by the lookup, for example, / (slash)
Get groups attributes	When selected, user group attributes are also looked up on the LDAP server to authenticate a user.
Base distinguished name to group objects	Distinguished name (DN) in the directory on the LDAP server where the lookup of group attributes should begin
Filter expression to locate a group object	Filtering term for restricting the lookup of group attributes To substitute the user name in the filtering term, *u%* is used as a variable.
Group attributes to retrieve	List of group attributes to retrieve from the LDAP server

RADIUS Specific Parameters

Settings for the RADIUS authentication method

Table 8-10 RADIUS Specific Parameters

Option	Definition
RADIUS server definition	List of RADIUS servers that authentication information is retrieved from
Default domain name	Name of the domain that information is retrieved from if no other domain is specified
Shared secret	Password used by the appliance to get access to the RADIUS server
Radius connection timeout in seconds	Time (in seconds) to elapse before the connection to the RADIUS server is closed if no traffic occurs
International text support	Set of characters used by default for a request sent from a client, for example, ISO-8859-1
Value of attribute with code	Code value for the attribute retrieved with the user group information, according to RFC 2865 For example, 25 is the code for the “class” attribute.
Vendor specific attribute with vendor ID	Vendor ID for retrieving vendor-related data in the search for user group information According to RFC 2865, the vendor ID is a part of the vendor attribute, followed by a number of subattributes. Its code value is 26.
Vendor subattribute type	Code value for the type of subattributes included in a vendor attribute. according to RFC 2865 Since not all vendors adhere to this structure, we recommend to specify 0 as value here. This allows the authentication module to retrieve all available vendor information.

Authentication Server Specific Parameters

Settings for the Authentication Server method

Table 8-11 Authentication Server Specific Parameters

Option	Definition
Authentication server URL	URL of the server used under this method to look up authentication information
Require client ID	When selected, the authentication server requires the ID of the client that a user sent a request from.

Table 8-11 Authentication Server Specific Parameters *(continued)*

Option	Definition
Store authentication result in a cookie	When selected, the information retrieved from the authentication server is stored in a cookie If cookie authentication is implemented, the cookie is added to the next request sent by the respective user, so that this user need not authenticate again.
Allow persistent cookie for the server	When selected, a cookie can be used persistently for sending multiple requests to the authentication server
Cookie TTL for the authentication server in seconds	Time (in seconds) that a cookie sent with a request to the server is stored
Cookie prefix	Prefix provided by the appliance for a cookie, for example, *MWG_Auth*

Implement a different authentication method

If you do not want to use the User Database authentication method of the default rule set, you can implement a different method, such as NTLM, LDAP, and others.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, navigate to the rule set that contains rules for authenticating users, for example, the default **Authentication and Authorize** rule set and select the nested **Authenticate with User Database** rule set.

The rules of the nested rule set appear on the settings pane.

3 Select the rule **Authenticate with User Database** and in the rule criteria click **User Database**.

The **Edit Settings** window opens.

4 From the list provided under **Authentication Method**, select an authentication method, for example, **NTLM**.

5 Configure common and specific parameters for the selected method as needed.

6 Click **OK** to close the window.

7 Click **Save Changes**.

We recommend that after changing the authentication method, you rename the settings of the Authentication module, the authentication rule, and the nested rule set, accordingly.

For example, after selecting NTLM, rename the settings to `NTLM` and both the rule and the nested rule set to `Authenticate with NTLM`.

Instead of renaming the default settings, you can also keep several settings with different names and parameter values for the Authentication module.

Using system settings to configure authentication

For some authentication methods, you need to configure settings that are not settings of the Authentication module, but of the appliance system.

This applies when you are implementing NTLM as the authentication method. In this case, you need to join the appliance to a Windows domain and configure the *Windows Domain Membership* settings, which are system settings.

It applies also for the Kerberos authentication method, which is implemented using the *Kerberos Administration* system settings.

Kerberos Administration settings

The Kerberos Administration settings are specific settings for the Kerberos authentication method.

Kerberos Administration

Settings for the Kerberos authentication method

Table 8-12 Kerberos Administration

Option	Definition
Key tab file	Input field for entering the file that contains the master key required to access the Kerberos server You can type a file name or use the **Browse** button to browse to the file and enter its name in the field. When a ticket is issued for authentication according to the Kerberos method, the master key is read on the appliance and used to verify the ticket. If you are running a load balancer that directs web requests to the appliance, tickets are issued for the load balancer and verified on the appliance. It is then not checked whether a request is directed to the appliance.
Kerberos realm	Administrative domain configured for authentication purposes Within the boundaries of this domain the Kerberos server has the authority to authenticate a user who submits a request from a host or using a service. The realm name is case sensitive, however. normally only uppercase letters are used, and it is good practice to make the realm name the same as that of the relevant DNS domain.
Maximal time difference between appliance and client	Maximal time (in seconds) that the system clocks on the appliance and its clients are allowed to differ Configuring Kerberos as the authentication method can lead to problems when particular browsers are used for sending requests: • When the Microsoft Internet Explorer is used in a version lower than 7.0, Kerberos authentication might not be possible at all. • When this explorer runs on Windows XP, Kerberos authentication might not work as expected. • When Mozilla Firefox is used, Kerberos authentication must be configured in the browser settings to enable this authentication method.
Enable replay cache	When selected, a ticket that is issued for authentication cannot be used more than once. Selecting this option reduces authentication performance

Join the appliance to a Windows domain

When using the NTLM authentication method, you need to join an appliance to a Windows domain to let the authentication module retrieve user information stored on the domain server.

An appliance can be joined to more than one domain.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to join and click **Windows Domain Memberhship**.

A list of domains appears on the settings pane. It is initially empty.

3 Click **Join** to enter a domain into the list.

The **Join Domain** window opens.

4 Configure a domain name, a domain controller, and other settings in the window.

5 Click **OK**.

The window closes and the new domain appears in the list. The appliance is now a member of this domain.

Repeat Steps 3 to 5 to add multiple domains.

Use the other icons on the toolbar to work with the list, for example. to modify a list entry or to let an appliance leave a domain.

See also

Windows Domain Membership settings on page 150

Windows Domain Membership settings

The Windows Domain Membership settings are used for joining an appliance to a Windows domain.

Join Domain

Settings for joining an appliance to a Windows domain

Table 8-13 Join Domain

Option	Definition
Windows domain name	Name of the domain
McAfee Web Gateway account name	Name of the account for an appliance
Overwrite existing account	When selected, an existing account is overwritten.
Use NTLM version 2	When selected, NTLM version 2 is used.
Timeout for requests to this NTLM domain	Time (in seconds) to elapse before processing of a request sent from the appliance to a domain controller stops if no response is received
Configured domain controllers	List of domain controllers that the appliance can connect to in order to retrieve authentication information Entries must be separated by commas.
Number of active domain controllers	Maximum number of configured domain controllers that can be active at the same time The allowed range is from 1 to 10.

Table 8-13 Join Domain *(continued)*

Option	Definition
Administrator name	User name for the account that is created when an appliance is joined to a domain. User name and password are only used for this purpose and not stored.
Password	Password for the administrator name

Authenticate and Authorize rule set

The Authenticate and Authorize rule set is the default rule set for authentication.

Default rule set – Authenticate and Authorize
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The rule set criteria specifies that the rule set applies when the protocol used on the connection for sending a request is HTTP or HTTPS.

The following rule sets are nested in this rule set:

- Authenticate with User Database
- Authorize

The rule set has also two rules of its own, which are processed before the nested rule sets.

Need to authorize Client IP?

Client.IP is in range list Unauthorized IPs –> Stop Rule Set –> Stop Rule Set

The rule uses the *Client.IP* property to check whether a request was sent from a client with an IP address that is in the range list for unauthorized IP addresses.

If this is the case, processing the rule set stops. No activities are then carried out to authenticate a user.

Processing continues with the next rule set.

The rule is not enabled by default.

Need to authorize URL?

URL is in list Unauthorized URLs –> Stop Rule Set –> Stop Rule Set

The rule uses the *URL* property to check whether a URL that access was requested is in the list of unauthorized URLs..

If this is the case, processing the rule set stops. No activities are then carried out to authenticate a user.

Processing continues with the next rule set.

The rule is not enabled by default.

Authenticate with User Database

This nested rule set asks unauthenticated users to authenticate. Its authentication method is retrieving information from the internal user database.

Nested default rule set – Authenticate with User Database
Criteria – *Connection.Protocol equals HTTP OR Connection.Protocol equals HTTPS*
Cycles – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user has not yet been authenticated or has undergone the authentication process, but authentication failed. .

The rule set contains the following rule.

Authenticate with User Database

Authentication.Authenticate<User Database> equals false–> Authenticate<Default>

The rule uses the *Authentication.Authenticate* property to check whether a user who sends a request for web access is authenticated. The settings that go with the property are the settings of the Authentication module. They specify that retrieving information from the internal user database on the appliance is used as the authentication method.

If a user has not been authenticated by information from the internal database, the rule applies and the Authenticate action is executed. Processing stops and a message is displayed, asking the user to authenticate. The settings of the action specify that the message is displayed with default values.

Processing continues when the next request is received on the appliance, which can be an authentication request by the same user.

Authorize

This nested rule allows only requests from users who are members of a whitelisted user group.

Nested default rule set – Authorize
Criteria – *Always*
Cycles – Requests (and IM)

The rule set contains the following rule.

Only allow users of Allowed User Groups

Authentication.UserGroups none in list Allowed User Groups–> Block<Authorized Only>

The rule uses the *Authentication.UserGroups* property to allow only users access who are members of a group on the specified whitelist.

If a user is not in one of the groups on the list, the rule applies and stops processing of all rules. The request is then not passed on to a web server.

The action settings specify that a notification is sent to the requesting user.

Processing continues with the next request.

Instant messaging authentication

Instant messaging authentication ensures that users of your network cannot access the web through an instant messaging service if they are not authenticated. The authentication process looks up user information and asks unauthenticated users to authenticate.

The following elements are involved in this process:

- Authentication rules that control the process
- The Authentication module, which retrieves information about users from different databases

An authentication rule can use an event to log information on the authentication of users who requested access to the web.

In this case, a logging module is also involved in the process.

Authentication rules

Instant messaging authentication is not implemented by default on the appliance, but you can import the *IM Authentication* rule set from the library.

This rule set contains a rule that looks up user information to see whether users who request web access are already authenticated. The method used for looking up the information is the User Database method.

Unauthenticated users that no information can be found for in the user database are asked to submit their credentials for authentication.

Another rule looks up information using the Authentication Server method to see whether users are authenticated and asks unauthenticated users for their credentials.

The Authentication module is called by these rules to retrieve the user information from the appropriate databases.

You can review the rules in the library rule set, modify or delete them, and also create your own rules.

Authentication module

The Authentication module (also known as *engine*) retrieves information that is needed to authenticate users from internal and external databases. The module is called by the authentication rules.

The different methods of retrieving user information are specified in the module settings. Accordingly, two different settings appear in the rules of the library rule set for instant messaging communication:

- User Database at IM Authentication Server
- Authentication Server IM

These settings are implemented with the rule set when it is imported from the library.

You can configure these settings, for example, to specify the server that user information is retrieved from under the Authentication Server method.

Logging module

The library rule set for instant messaging authentication includes a rule that logs authentication-related data, such as the user name of a user who requested web access, or the URL of the requested web object.

The logging is handled by the FileSystemLogging module, which you can also configure settings for.

Configure instant messaging authentication

You can implement instant messaging authentication and adapt it to the needs of your network.

Complete the following high-level steps.

Task

1. Import the IM Authentication rule set from the library.
2. Review the rules in the rule set and modify them as needed.

You can, for example, do the following:

- Modify the settings of the Authentication module for the User Database or the Authentication Server method.
- Modify the settings of the logging module that handles the logging of information about instant messaging authencation.

3 Save your changes.

Configure the Authentication module for instant messaging authentication

You can configure the Authentication module to specify how it retrieves the information that is needed to authenticate users of an instant messaging service.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select the rule set for instant message authentication.

If you have imported this rule set from the library, it is the *IM Authentication* rule set.

The rules of the rule set appear on the settings pane.

3 Make sure **Show details** is selected.

4 Find the rules that call the Authentication module.

In the library rule set, these are the rules *Authenticate Clients against the User Database* and *Redirect Not Authenticated Clients to the Authentication Server*.

5 In the rule criteria, click the settings name of the settings you want to configure.

This name appears next to the *Authentication. Authenticate* property.

In the library rule set, it is the *User Database at IM Authentication Server* or the *Authentication Server IM* settings.

The **Edit Settings** window opens. It provides the settings for the Authentication module.

6 Configure these settings as needed.

7 Click **OK** to close the window.

8 Click **Save Changes**.

See also

Authentication settings on page 142

Configure the File System Logging module for instant messaging authentication

You can configure the File System Logging module to specify how it logs information that is related to instant messaging authentication.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, select the rule set for instant message authentication.

   If you have imported this rule set from the library, it is the *IM Authentication* rule set.

   The rules of the rule set appear on the settings pane.
3. Make sure **Show details** is selected.
4. Find the rule that calls the File System Logging module.

   In the library rule set , this is the rule *Show Authenticated page* .
5. In the rule event, click the name of the settings for the module.

   In the library rule set, this name is *IM Logging*.

   The **Edit Settings** window opens. It provides the settings for the File System Logging module.
6. Configure these settings as needed.
7. Click **OK** to close the window.
8. Click **Save Changes**.

See also

File System Logging settings on page 348

IM Authentication rule set

The IM Authentication rule set is a library rule set for instant messaging authentication.

Library rule set – IM Authentication
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The following rule sets are nested in this rule set:

- IM Authentication Server
- IM Proxy

IM Authentication Server

This nested rule set handles authentication for instant messaging users. It applies the User Database method for retrieving user information.

Nested library rule set – IM Authentication Server
Criteria – *Authentication.IsServerRequest equals true*
Cycles – Requests (and IM), responses, embedded objects

The rule set criteria specifies that the rule set applies when authentication has been requested for a user of an instant messaging service.

The rule set contains the following rules.

Authenticate clients against user database

Authentication.Authenticate<User Database at IM Authentication server> equals false–> Authenticate<IM Authentication>

The rule uses the *Authentication.Authenticate* property to check whether a user who sends a chat message or file under an instant messaging protocol is authenticated. The settings that follow the property in the rule criteria specify the User Database method for this authentication.

If a user is not authenticated under this method, processing stops and a message is displayed asking the user to authenticate.

The action settings specify that the IM Authentication template is used for displaying the authentication message to the user.

Processing continues when the next user request is received.

Show Authenticated page

Always–> Redirect<Show IM Authenticated> —

Set User-Defined.logEntry =

“[”

+ DateTime.ToISOString

+ “]””

+ URL.GetParameter (“prot”)

+ ““auth””

+ Authentication.Username

+ ““ ””

+ URL.GetParameter (“scrn”)

+ ““““

FileSystemLogging.WriteLogEntry (User-Defined.logEntry)<IM Logging>

The rule redirects a request sent from a client by an instant messaging user to an authentication server and displays a message to inform the user about the redirect.

The action settings specify that the Show IM Authenticated template is used for the message.

The rule also uses an event to set values for a log entry on the authentication request. It uses a second event to write this entry into a log file. A parameter of this event specifies the log entry.

The event settings specify the log file and the way it is maintained.

IM Proxy

This nested rule set handles authentication of instant messaging users. It applies the Authentication Server method to retrieve user information.

Nested library rule set – IM Proxy
Criteria – *Connection.Protocol.IsIM equals true AND IM.MessageCanSendBack is true*
Cycles – Requests (and IM), responses, embedded objects

The rule set criteria specifies that the rule set applies when a user sends a chat message or a file on a connection under an instant messaging protocol and a message can already be sent back from the appliance to the user.

The rule set contains the following rule.

Redirect not authenticated users to the authentication server

Authentication.Authenticate<Authentication Server IM> equals false–> Authenticate<IM Authentication>

The rule uses the *Authentication.Authenticate* property to check whether a user who sends a chat message or file under an instant messaging protocol is authenticated. The settings that follow the property in the rule criteria specify the Authentication Server method for this authentication.

If a user is not authenticated under this method, processing stops and a message is displayed, asking the user to authenticate.

The action settings specify that the IM Authentication template is used for displaying the authentication message to the user.

Processing continues when the next user request is received.

Client Certificate authentication

Submitting a client certificate can be configured as a method of accessing the user interface of the appliance. This method is known as *Client Certificate authentication* or *X.509 authentication*.

Client Certificate authentication is one of the methods you can choose for the authentication procedure when configuring the proxy functions of the appliance.

The following applies to the method when using it in proxy configuration.

- No user name and password is required to authenticate a user who sends a request, as is the case with other methods such as NTLM or LDAP.
- The method can be implemented for requests that are sent in SSL-secured communication from a web browser on a client to an appliance that is configured in explicit proxy mode.
- The protocol used for this communication is HTTPS.

A client certificate is submitted when the SSL handshake is performed as one of the initial steps in the communication between the appliance and a client. The request is then redirected to an authentication server to validate the certificate.

If it is valid, authentication is successfully completed for the client and the request is eventually forwarded to the appropriate web server.

When running multiple appliances as nodes in a configuration, it is important that the authentication server resides on the node that a request was originally directed to.

Also forwarding to the web after successful authentication must be done from the same node.

Use of an authentication server for Client Certificate authentication is controlled by rules. You can import an authentication server rule set and modify the rules in its nested rule sets to enable the use of appropriate certificates.

You must also implement a way to let Client Certificate authentication be applied. A recommended way of doing this is using cookie authentication.

If this method is implemented, authentication is required for a client that a request was sent from, but a cookie is set for this client after a certificate has been submitted and recognized as valid once. Submitting a certificate is then not required for subsequent requests from that client.

You can import and modify a rule set for having Client Certificate authentication handled in this way.

Use of certificates for Client Certificate authentication

Different types of certificates are required for performing authentication under the Client Certificate authentication method, which can be implemented for SSL-secured communication.

Client certificate

A client certificate is needed to certify the identity of a client that sends a request to the appliance.

Only if the client is trusted will a request that it sends be accepted. A client ist trusted if the certificate that is submitted with the request has been signed by a Root CA (certificate authority) that is trusted.

Under the Client Certificate authentication method, the client certificate is also used for authentication. Authentication is successfully completed if the client certificate that is submitted with a request has been signed by a trusted certificate authority.

Server certificate

A server certificate is needed to certify the identity of a server that is involved in SSL-secured communication.

A server is trusted by a client if the certificate that it sends during the initial steps of the communication has been signed by a Root CA (certificate authority) that is also trusted by the client.

Under the Client Certificate authentication method, a server certificate is needed for the authentication server.

Root CA

A Root CA (certificate authority) is an instance that signs other certificates.

In SSL-secured communication, a Root CA appears itself as a certificate that can be viewed in the communication process.

If a Root CA is trusted by a client or server, certificates that have been signed by it are trusted as well, which means that if a client or server submits such a signed certificate, it is trusted.

Rule sets for Client Certificate authentication

Rule sets for implementing the Client Certificate authentication method are available in the rule set library.

Authentication Server (for X509 Authentication) rule set

The Authentication Server (for X509 Authentication) rule set uses several nested rule sets to handle use of the authentication server under the Client Certificate authentication method.

- **SSL Endpoint Termination** — Prepares the handling of requests in SSL-secured communication
  - **Accept Incoming HTTPS Connections** — Provides the certificates that can be submitted for the authentication server
  - **Content Inspection** — Enables inspection of the content that is transmitted with a request

- **Authentication Server Requests** — Redirects requests back to the proxy on the appliance for further processing after authentication on the authentication server was completed successfully

  Requests are also redirected if a cookie has been set for a client that a request was sent from.

  If authentication could not be completed successfully on the authentication server, the user is asked to submit credentials for authentication on the user database.

- **Block All Others** — Blocks requests for which authentication was not completed successfully

Cookie Authentication (for X509 Authentication) rule set

The Cookie Authentication (for X509 Authentication) rule set uses several nested rule sets to initiate use of the Client Certificate authentication method and handle the setting of cookies.

- **Cookie Authentication at HTTP(S) Proxy** — Contains nested rule sets that handle Client Certificate authentication with cookies
  - **Set Cookie for Authenticated Clients** — Sets a cookie after authentication has been successfully completed once for a client and redirects the request that the client sent back to the proxy on the appliance for further processing
  - **Authenticate Clients with Authentication Server** — Redirects requests sent from clients for which no cookie has been set to the authentication server

Redirecting requests to an authentication server

Under the Client Certificate authentication method, a request is redirected to an authentication server for validating the client certificate that was submitted with it. The redirecting can be done using a special listener port on the appliance or a unique host name.

Using a special listener port

Requests can be redirected to an authentication server using a special listener port, for example, port 444. Suppose the IP address of an appliance is 192.168.122.119, then a request will be redirected to the authentication server by:

```
https://192.168.122.119:444/
```

However, it is important to consider whether exceptions from using a proxy have been configured for the web browser on a client that sends the request.

- **No proxy exceptions configured** — If no proxy exceptions have been configured, all requests are sent to the proxy port that is listening for them on the appliance, which is port 9090 by default.

  Even a request to `https://192.168.122.119:444/` will arrive on port 9090 if this is the configured proxy port.

  If a firewall is part of your network configuration, no exceptions from the firewall rules are needed because there is no connection from the client to port 444.

  To ensure requests are redirected to the authentication server, 444, or another value that you want to use for this purpose, must be configured for the *URL.Port* property in the criteria of the Authentication Server (for X509 Authentication) rule set.

  The value of the URL.Port property is the port contained in the URL that is specified by a request. It can be, for example, 444, even if the request actually arrives at port 9090.

- **Proxy exceptions configured** — Proxy exceptions can be configured for various reasons. For example, a web browser could be configured not to use proxies for accessing local hosts.

  A request to `https://192.168.122.119:444/` will then not arrive at port 9090.

  Because the browser is configured to access its destination directly, it will try to connect to the appliance on port 444. This means that you need to set up a listener port with port number 444.

  If firewall rules are in place, an exception is also needed to allow requests to arrive at port 444.

  To ensure requests are processed by the appropriate rules, 444, or another value that you want to use for this purpose, must be configured for the *Proxy.Port* property in the criteria of the Authentication Server (for X509 Authentication) rule set.

  The value of the Proxy.Port property is the port that a request actually arrives at. It is, for example, 444 if you have set up a port with this number for receiving requests that are to be redirected to an authentication server.

Using a unique host name

Requests can be redirected to an authentication server using a unique host name, for example, authserver.local.mcafee. Using this name, requests are redirected to the authentication server by:

```
https://authserver.mcafee.local
```

The client that the request was sent from must not try to look up the host name using DNS, as the URL will most likely not resolve and the client will be unable to connect.

To ensure that requests are processed by the appropriate rules, this host name must be configured as the value for the *URL.Host* property in the criteria of the Authentication Server (for X509 Authentication) rule set.

Implement Client Certificate authentication

The Client Certificate authentication method uses client certificates that are sent with requests for authentication. To implement this method on the appliance, complete the following high-level steps.

Task

1. Import the Authentication Server (for X509 Authentication) rule set.
2. Modify the nested rule sets to configure the use of appropriate certificates.

3 Configure a listener port for requests sent by web browsers that are not using the proxy port on the appliance.

4 Configure a way to let Client Certificate authentication be applied.

You can import and modify the Cookie Authentication (for X509 Authentication) rule set to use a cookie for authentication after Client Certificate authentication has been applied once and successfully been completed.

5 Make sure a suitable client certificate is available on a web browser that is used for sending requests to the appliance.

Import the Authentication Server (for X509 Authentication) rule set

To implement the Client Certificate authentication method on the appliance, there must be a rule set that handles authentication in this way. You can import the Authentication Server (for X509 Authentication) rule set for this purpose.

We recommend that you insert the rule set at the top of the rule sets tree.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, navigate to the position where you want to insert the rule set and click **Add**.

3 Click **Top Level Rule Set**, then click **Import Rule Set from Library**.

The **Add from Rule Set Library** window opens.

4 Select the **Authentication Server (for X509 Authentication)** rule set and click **OK**.

If conflicts arise from the import, they are displayed next to the list of rule sets. Follow one of the suggested procedures for solving them before clicking OK.

The rule set is inserted with its nested rule sets in the rule sets tree.

5 Review the rule set criteria and modify them if necessary.

After the import, the criteria is:

URL.Port equals 444 or Proxy.Port equals 444.

This ensures that the rule set is applied to all requests coming in on that port. If you want to use a different port, specify its port number here.

Modify a rule set to configure the use of server certificates

The Authentication Server (for X509 Authentication) rule set needs to be modified to ensure appropriate server certificates are submitted for the authentication server. The modification is done in a nested rule set.

Because it is possible to reach the authentication server under different host names and IP addresses, you can let the appliance submit a different server certificate each time, so that the host name or IP address is matched by the common name in the certificate.

To achieve this, you need to import a server certificate for each host name or IP address and add it to the list of server certificates.

Task

1 Select **Policy** | **Rule Sets** and expand the **Authentication Server (for X509 Authentication)** rule set.

2 Expand the nested **SSL Endpoint Termination** rule set and, within this rule set, click the nested **Accept Incoming HTTPS Connections** rule set.

3 In the **Set client context** rule, click the **Proxy Certificate** event settings.

The **Edit Settings** window opens.

4 In the **Define SSL Context** section, review the list of server certificates.

5 To add a server certificate to the list:

a Click the **Add** icon above the list.

The **Add Host to Certificate Mapping** window opens.

b In the **Host** field, enter the host name or IP address that the certificate should be submitted for.

c Click **Import**.

The **Import Server Certificate** window opens.

d Click **Browse** and browse to the certificate you want to import.

e Repeat this activity to import a key and certificate chain with the certificate.

f Click **OK**.

The window closes and the import is performed. The certificate information appears in the **Add Host to Certificate Mapping** window.

6 [Optional] In the **Comment** field, type a plain-text comment on the server certificate.

7 Click **OK**.

The window closes and the server certificate appears in the list.

8 Make sure the **SSL-Scanner functionality applies only to client connection** checkbox is selected.

This lets the appliance accept requests from its clients without contacting other servers of the network, which is not required in this communication.

9 Click **OK** to close the **Edit Settings** window.

10 Click **Save Changes**.

Modify a rule set to configure the use of certificate authorities

The Authentication Server (for X509 Authentication) rule set needs to be modified to ensure appropriate Root CAs (certificate authorities) are configured. The modification is done in a nested rule set.

A client certificate is trusted if signed by a certificate authority from the list that is maintained on the appliance. You need to import all certificate authorities into the list that you want to be signing instances for trusted client certificates.

Task

1 Select **Policy | Rule Sets** and expand the **Authentication Server (for X509 Authentication)** rule set.

2 Expand the nested **SSL Authentication Server Request** rule set.

3 In the **Ask user for client certificate** rule, click the **X509 Auth** module settings.

The **Edit Settings** window opens.

4 In the **Client Certificate Specific Parameters** section, review the list of certificate authorities.

5 To add a certificate authority to the list:

a Click the **Add** icon above the list.

The **Add Certificate Authority** window opens.

b In the **Host** field, enter the host name or IP address that the certificate should be submitted for.

c Click **Import**.

A window providing access to your local file system opens.

d Browse to the certificate authority file you want to import.

e Click **OK**.

The window closes and the import is performed. The certificate appears in the **Add Certificate Authority** window.

6 Make sure the **Trusted** checkbox is selected.

7 [Optional] In the **Comment** field, type a plain-text comment on the certificate authority.

8 Click **OK**.

The window closes and the certificate authority appears in the list.

9 Click **OK** to close the **Edit Settings** window.

10 Click **Save Changes**.

Configure a listener port for incoming requests on the appliance

Requests that are sent to the appliance can be received on the proxy port or a special listener port. The proxy port is port 9090 by default.

You need to configure a listener port if proxy exceptions have been created that prevent requests from arriving at the proxy port.

Task

1 Select **Configuration | Appliances**.

2 On the appliances tree, select the appliance you want to configure a listener port on and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

The proxy settings appear on the settings pane.

3 Scroll down to the **HTTP Proxy** section.

4 Make sure **Enable HTTP proxy** is selected.

5 On the toolbar of the **HTTP port definition list**, click the **Add** icon.

The **Add HTTP Proxy Port** window opens.

6 Configure a listener port as follows:

a In the **Listener address** field, type `0.0.0.0:444`.

If you want to use a different port for listening to incoming requests, type it here.

b In the **Ports treated as SSL** field, type `*`.

c Make sure all other checkboxes are selected.

7 Click **OK** to close the **Edit Settings** window.

8 Click **Save Changes**.

9 Restart the appliance to make the configuration of the listener port effective.

Import the Cookie Authentication (for X509 Authentication) rule set

When the Client Certificate authentication method is used on the appliance, use of this method can be initiated by the Cookie Authentication (for X509 Authentication) rule set.

We recommend that you insert this rule set after the rules sets for functions that do not require authentication, but before the rule sets that handle the filtering functions.

This ensures the filtering functions are not executed when a request is blocked because authentication failed, which saves resources and improves performance.

If your rule set system is similar to the default system, you can insert the rule set after the SSL Scanner and Global Whitelist rule sets, but before the Content Filtering and Gateway Antimalware rule sets.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, navigate to the position where you want to insert the rule set and click **Add**.

3 Click **Top Level Rule Set**, then click **Import Rule Set from Library**.

The **Add from Rule Set Library** window opens.

4 Select the **Cookie Authentication (for X509 Authentication)** rule set and click **OK**.

If conflicts arise from the import, they are displayed next to the list of rule sets. Follow one of the suggested procedures for solving them before clicking OK.

The rule set is inserted with its nested rule sets in the rule sets tree.

Modify a rule set to change the listener port for incoming requests

You can modify the Cookie Authentication (for X509 Authentication) rule set to configure a listener port for incoming requests that you want to use instead of port 444, which is the default port. The modification is done in a nested rule set.

A special listener port must be used for receiving incoming requests if proxy exceptions are in place that prevent requests from arriving at the proxy port of the appliance. Requests that arrive at port 444 or a different port you have configured for this purpose are redirected to the authentication server.

Task

1 Select **Policy** | **Rule Sets** and expand the **Cookie Authentication (for X509 Authentication)** rule set.

2 Expand the nested **Cookie Authentication at HTTP(S) Proxy** rule set and, within this rule set, click the nested **Authenticate Clients with Authentication Server** rule set.

3 In the **Set client context** rule, click the **Proxy Certificate** event settings.

The **Edit Settings** window opens.

4 In the **Authentication Server Specific Parameters** section, review the URL in the **Authentication server URL** field.

The URL is by default as follows:

```
https://$<propertyInstance useMostRecentConfiguration="false" propertyId=
"com.scur.engine.system.proxy.ip"/>$:444
```

When the rule is processed, the `$...$` term is replaced by the IP address of the appliance.

5 To configure a different listener port, type the number of this port here.

6 Click **OK** to close the **Edit Settings** window.

7 Click **Save Changes**.

Import a client certificate into a browser

A suitable client certificate must be available on a web browser to be sent with a request to an appliance in SSL-secured communication.

Procedures for importing certificates vary for different browsers and are subject to change. Browser menus can also vary depending on the operating system you are using.

The following are two possible procedures for importing a client certificate into Microsoft Internet Explorer and Mozilla Firefox.

Tasks

- *Import a client certificate into Microsoft Internet Explorer* on page 165
  You can import a client certificate and make it available on Microsoft Internet Explorer for presenting it in SSL-secured communication.
- *Import a client certificate into Mozilla Firefox* on page 166
  You can import a client certificate and make it available on Mozilla Firefox for presenting it in SSL-secured communication.

Import a client certificate into Microsoft Internet Explorer

You can import a client certificate and make it available on Microsoft Internet Explorer for presenting it in SSL-secured communication.

> **Before you begin**
>
> To import the certificate file, you must have stored it within your local file system.

Task

1 Open the browser and on the top-level menu bar, click **Tools**, then click **Internet Options**.

The **Internet Options** window opens.

2 Click the **Content** tab.

3 In the **Certificates** section, click **Certificates**.

The **Certificates** window opens.

4 Click **Import**.

The Certificate Import Wizard appears.

5 On the wizard pages, proceed as follows:

a On the **Welcome** page, click **Next**.

b On the **File to Import** page, click **Browse** and navigate to the location where you stored the certificate file.

c In the **File Name** field, type `*.pfx`, then press **Enter**.

d Select the certificate file and click **Open**, then click **Next**.

e On the **Password** page, type a password in the **Password** field. Then click **Next**.

f On the **Certificate Store** page, click **Place all certificates in the following store**.

g In the **Certificate Store** section on the same page, select **Personal**, then click **Next**.

h On the **Completing the Certificate Import Wizard** page, click **Finish**.

6 Confirm the message that appears by clicking **OK**.

7 Click **Close**, then click **OK** to close the **Certificates** and **Internet Options** windows.

Import a client certificate into Mozilla Firefox

You can import a client certificate and make it available on Mozilla Firefox for presenting it in SSL-secured communication.

> **Before you begin**
> To import the certificate file, you must have stored it within your local file system.

Task

1 Open the browser and on the top-level menu bar, click **Tools**, then click **Options**.

The **Options** window opens.

2 Click **Advanced**, then click **Encryption**.

3 In the **Certificates** section of the **Encryption** tab, click **View Certificates**.

The **Certificate Manager** window opens.

4 Click **Import**.

Your local file manager opens.

5 Navigate to the certificate file that you have stored and click **Open**.

6 When prompted, submit a password, then click **OK**.

Administrator accounts

Administrator accounts can be set up and managed on the appliance or on an external server. Roles can be created with different access privileges for administrators.

Add an administrator account

You can add administrator accounts to the account that is created by the appliance system at the initial setup.

Task

1 Select **Accounts** | **Administrator Accounts**.

2 Under **Internal Administrator Accounts**, click **Add**.

The **Add Administrator** window opens.

3 Add a user name, a password, and other settings for the account. Then click **OK**.

The window closes and the new account appears in the accounts list.

4 Click **Save Changes**.

See also
Administrator account settings on page 168

Edit an administrator account

You can edit administrator accounts including the one that is created by the appliance system at the initial setup.

Task

1 Select **Accounts** | **Administrator Accounts**.

2 Under **Internal Administrator Accounts**, select an account and click **Edit**.

Before selecting an account, you can type a filtering term in the **Filter** field to display only accounts with matching names.

The **Edit Administrator** window opens

3 Edit the settings of the account as needed. Then click **OK**.

The window closes and the account appears with your changes in the accounts list.

4 Click **Save Changes**.

See also
Administrator account settings on page 168

Delete an administrator account

You can delete any administrator account, as long as there is at least one that remains.

Task

1. Select **Accounts** | **Administrator Accounts**.
2. Under **Internal Administrator Accounts**, select an account and click **Delete**.

   Before selecting an account, you can type a filtering term in the **Filter** field to display only accounts with matching names.

   A window opens to let you confirm the deletion.
3. Click **Save Changes**.

Administrator account settings

The administrator account settings are used for configuring credentials and roles for administrators.

Administrator account settings

Settings for administrator accounts

Table 8-14 Administrator account settings

Option	Definition
User name	User name of an administrator
Password	Administrator password
Password repeated	Repetition of the password to check and confirm it In the Edit Administrator window, you need to select **Set a new password** before the two password fields become available.
Role	List for selecting an administrator role You can use the **Add** and **Edit** options to add and edit roles. The addted and edited roles appear in the list of administrator roles.
Name	Real name of the person that an account is set up for Configuration of this name is optional.

Test with current settings

Settings for testing whether an administrator with given credentials would be admitted on the appliance

Table 8-15 Test with current settings

Option	Definition
User	User name that is tested
Password	Tested password
Test	Executes the test. The **Authentication Test Results** window opens to display the outcome of the test.

Manage administrator roles

You can create roles and use them for configuring administrator accounts.

One administrator role is already created by the appliance system at the initial setup.

Task

1 Select **Accounts** | **Administrator Accounts**.

2 To add an administrator role:

   a Under **Roles**, click **Add**.

   The **Add Role** window opens.

   b In the **Name** field, type a role name.

   c Configure access rights for the dashboard, rules, lists, and other items.

   d Click **OK**.

   The window closes and the new role appears in the list of administrator roles.

3 Use the **Edit** and **Delete** options in similar ways to edit and delete roles.

4 Click **Save Changes**.

The newly added or edited role is now available for being assigned to an administrator account.

See also
Administrator role settings on page 169

Administrator role settings

The administrator role settings are used for configuring roles that can be assigned to administrators.

Administrator role settings

Settings for administrator roles

Table 8-16 Administrator role settings

Option	Definition
User name	User name of an administrator
Password	Administrator password
Password repeated	Repetition of the password to check and confirm it In the **Edit Administrator** window, you need to select **Set a new password** before the two password fields become available.
Role	List for selecting an administrator role You can use the **Add** and **Edit** options to add and edit roles. The added and edited roles appear in the list of administrator roles.
Name	Real name of the person that the account is set up for Configuring this name is optional.

Configure external account management

You can let administrator accounts be managed on external authentication servers and map externally stored user groups and individual users to roles on an appliance.

Task

1. Select **Accounts** | **Administrator Accounts**.
2. Click **Administrator accounts are managed in an external directory server**.

   Additional settings appear.
3. Under **Authentication Server Details**, configure settings for the external server.

   These settings determine the way the Authentication module on the appliance retrieves information from that server.
4. Use the settings under **Authentication group = role mapping**, to map user groups and individual users stored on the external server to roles on the appliance:

   a. Click **Add**.

      The **Add Group/User Role Name Mapping** window opens.

   b. Select the checkboxes next to the field for group or user matching as needed and type the name of a group or user in this field.

   c. Click **OK**.

   d. Under **Role to map to**, select a role.

   e. Click **OK**.

      The window closes and the new mapping appears on the mappings list.

   f. Click **Save Changes**.

   You can use the **Edit** and **Delete** options in similar ways to edit and delete mappings.

9 Quota management

Quota management is a means of guiding the users of your network in their web usage. This way you can ensure that resources and performance of your network are not impacted in excess.

Quotas and other restrictions can be imposed in several ways:

- **Time quotas** — Limit the time that users are allowed to spend on their web usage
- **Volume quotas** — Limit the volume that users are allowed to consume during their web usage
- **Coaching** — Limits the time that users can spend on their web usage, but allows them to exceed the configured time limit if they choose to do so
- **Authorized override** — Limits the time that users can spend on web usage in the same way as coaching

  However, the time limit can only be exceeded by an action of an authorized user, for example, a teacher in a classroom.
- **Blocking sessions** — Blocks access to the web for a configured period of time after a user attempted to access a web object, for which access was not allowed

Quotas and other restrictions can be imposed separately or in a combination of measures.

Contents

Imposing quotas and other restrictions on web usage

By imposing quotas and other restrictions you can guide web usage and limit the consumption of network resources.

The following elements are involved in this process:

- Quota management rules that control the process
- Quota management lists that are used by the rules to impose restrictions with regard to users and particular web objects, such as URLs, IP addresses, and others
- Quota management modules, which are called to handle time and volume quotas, session times, and other parameters of the process

Quota management rules

The rules that control the management of quotas and other restrictions are contained in different rule sets, according to the type of restriction, for example, in a time quota or a coaching rule set.

The rules in these rule sets check whether the configured limits for time or and volume have been exceeded and eventually block requests for further web access. They also redirect requests when a user chooses to continue with a new session.

Quota management rule sets are not implemented in the default rule set system, but can be imported from the rule set library. The library rule set names are *Time Quota*, *Volume Quota*, *Coaching*, *Authorized Override*, and *Blocking Sessions*.

You can review the rules that are implemented with the library rule sets, modify or delete them, and also create your own rules.

Quota management lists

The rule sets for managing quotas and other restrictions use lists of web objects and users to impose restrictions accordingly. The lists are contained in the criteria of a rule set.

For example, a list contains a number of URLs and the time quota rule set has this list in its criteria. Then this rule set and the rules within it apply only if a user accesses one of the URLs on the list. Lists of IP addresses or media types can be used in the same way.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the quota management rule sets.

Quota management modules

The quota management modules (also known as *engines*) handle the time and volume parameters of the quota management process and are checked by the rule sets of the process to find out about consumed and remaining times or volumes, session times, and other values.

There is a module for each type of restriction, for example, the *Time Quota* or the *Coaching* module.

By configuring settings for these modules, you specify the times and volumes that apply in the quota management process. For example, when configuring the time quota module, you specify how much hours and minutes per day users can access web objects with particular URLs or IP addresses.

Session time

Among the settings that you can configure for the quota management module is also *session time*. This is the time allowed for a single session that a user spends on web usage.

Session time is configured separately and handled differently for time quotas, volume quotas, and other parameters of the quota management process.

- **Session time for time quotas** — When configuring time quotas, you also need to configure a session time. Whenever session time has elapsed for a user, the amount of time that is configured as session time is deducted from the user's time quota.

  As long as the time quota has not been used up, the user can start a new session. When the time quota has elapsed, a request that the user sends is blocked and a block message is displayed.

- **Session time for volume quotas** — When configuring volume quotas, the session time has no impact on the volume quota for a user.

  You can still configure a session time to inform the user about the amount of time that has been used up for web access. When time has elapsed for a session, the user can start a new session, as long as the configured volume has not been consumed.

  If you set the session time to zero, no session time is configured and communicated to the user.

- **Session time for other quota management functions** — Session time can also be configured for other Coaching, Authorized Override, and Blocking Sessions. Accordingly, there can be a coaching, an authorized override, or a blocking session.

  When session time has elapsed for coaching and authorized overriding, a request that a user sends is blocked.

  A message is displayed to the user, stating why the request was blocked. The user can start a new session unless time quota has also been configured and is used up.

  The session time that is configured for a blocking session is the time during which requests sent by a particular user are blocked. When this time has elapsed, requests from the user are again accepted unless time quota has also been configured and is used up.

Combining quota management functions

Using a particular quota management function to restrict web usage has no impact on the use of other quota management functions. For example, time quotas and volume quotas are configured and implemented separately on the appliance.

You can, however, combine these functions in meaningful ways.

For example, you can impose coaching on users' access to some URL categories, while requesting authorized override credentials for others.

For still another group of categories you could block users who attempt to access them over a configured period of time.

Time quota

By configuring time quotas, you can limit the time that users of your network are allowed to spend for web usage.

Time quotas can be related to different parameters:

- **URL categories** — When time quotas are related to URL categories, users are allowed only a limited time for accessing URLs that fall into particular categories, for example, Online Shopping.
- **IP addresses** — When time quotas are related to IP addresses, users who send requests from particular IP addresses are allowed only a limited time for web usage.
- **User names** — When time quotas are related to user names, users are allowed only a limited time for web usage. Users are identified by the user names they submitted for authentication on the appliance.

These parameters are used by the rules in the library rule set for time quotas. You can create rules of your own that use other parameters in relation to time quotas.

The time that users spend on web usage is stored on the appliance. When the configured time quota has been exceeded for a user, a request that this user sends is blocked. A message is displayed to the user stating why the request was blocked.

Users are identified by the user names they submitted for authentication. If no user name is sent with a request, web usage is recorded and blocked or allowed for the IP address of the client system that the request was sent from.

Web usage can be limited to time spent per day, per week, or per month.

Configure time quotas

You can configure time quotas to limit the time users of your network spend on web usage.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, expand the rule set that contains rules for time quotas, for example, the **Time Quota** library rule set.

   The nested rule sets appear.
3. Select the appropriate nested rule set.

   For example, to configure time quotas with regard to URL categories, select **Time Quota With URL Configuration**.

   The general settings and rules of the rule set appear on the settings pane.
4. In the rule set criteria, click the **URL Category Block List for Time Quota** list name.

   A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

   The **Edit List (Category)** window opens.
5. Add URL categories to the blocking list. Then click **OK** to close the window.
6. In the criteria for one of the rules, click the **URL Category Configuration** settings name.

   The **Edit Settings** window opens.

7 Configure session time and the time quota per day, week, and month. Then click **OK** to close the window.

8 Click **Save Changes**.

See also

Time Quota settings on page 175

Time Quota settings

The Time Quota settings are used for configuring the module that handles time quota management.

Time Quota per Day, Week, Month, and Session Time

Settings for time quotas

When a time unit or the session time is selected, the heading of the next section reads accordingly.

Table 9-1 Time Quota per Day, Week, Month, and Session Time

Option	Definition
Time quota per day (week, month)	When selected, the quota that is configured in the next section applies to the selected time unit.
Session time	When selected, the quota that is configured in the next section applies to the session time.

Hours and Minutes for . . .

Settings for time quotas that apply to the selected time unit or the session time

The heading of this section varies according to what you selected in the preceding section.

For example, if you selected *Time quota per week*, the heading reads *Hours and Minutes for Time Quota per Week*.

Table 9-2 Hours and Minutes for . . .

Option	Definition
Hours	Allowed hours per day, week, month, or for the session time
Minutes	Allowed minutes per day, week, month, or for the session time

Actual Configured Time Quota

Displays the configured time quotas.

Table 9-3 Actual Configured Time Quota

Option	Definition
Time quota per day (week, month)	Allowed time per day, week, or month
Session time	Allowed session time

Time Quota rule set

The Time Quota rule set is a library rule set for imposing time quotas on web usage.

Library rule set – Time Quota
Criteria – *SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Time Quota With URL Configuration
- Time Quota With IP Configuration

  This rule set is not enabled initially.
- Time Quota With Authenticated User Configuration

  This rule set is not enabled initially.

Time Quota With URL Configuration

This nested rule set handles time quotas related to URL categories.

Nested library rule set – Time Quota With URL Configuration
Criteria – *URL.Categories<Default> at least one in list URL Categories Blocklist for Time Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for time quotas related to URL categories.

The rule set contains the following rules:

Redirecting after starting new time session

Quota.Time.IsActivationRequest equals true –> Redirect<Redirection After Time Session Activation>

The rule redirects a request to let a user again access a web object after session time has been exceeded and the user has chosen to continue with a new session.

The action settings specify a message to the requesting user.

Check if time session has been exceeded

Quota.Time.Session.Exceeded<URL Category Configuration> equals true –> Block<ActionTimeSessionBlocked>

The rule uses the *Quota.Time.SessionExceeded* property to check whether the configured session time has been exceeded for a user. If it has, the user's request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles time quotas.

The action settings specify a message to the requesting user.

Check if time quota has been exceeded

Quota.Time.Exceeded<URL Category Configuration> equals true –> Block<ActionTimeQuotaBlocked>

The rule uses the *Quota.Time.Exceeded* property to check whether the configured time quota has been exceeded for a user. If it has, the user's request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles time quotas.

The action settings specify a message to the requesting user.

Time Quota With IP Configuration

This nested rule set handles time quotas related to IP addresses.

Nested library rule set – Time Quota With IP Configuration
Criteria – *Client.IP is in list IP Blocklist for Time Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for time quotas related to IP addresses.

The rules in this rule set are the same as in the Time Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *IP Configuration*.

Time Quota With Authenticated User Configuration

This nested rule set handles time quotas related to user names.

Nested library rule set – Time Quota With Authenticated User Configuration
Criteria – *Authenticated.RawUserName is in list User Blocklist for Time Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for time quotas related to user names.

The rules in this rule set are the same as in the Time Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *Authenticated User Configuration*.

Volume quota

By configuring volume quotas, you can limit the volume of web objects, measured in GB and MB, that the users of your network are allowed to download from the web.

Volume quotas can be related to several parameters:

- **URL categories** — Users are allowed to download only a limited volume of web objects through URLs that fall into particular categories, for example, Streaming Media.
- **IP addresses** — Users who send download requests from particular IP addresses are allowed only a limited volume.
- **User names** — Users are allowed to download web objects only up to a limited volume. Users are identified by the user names they submitted for authentication on the appliance.
- **Media types** — Users are allowed to download web objects belonging to particular media types only up to a limited volume.

These parameters are used by the rules in the library rule set for volume quotas. You can create rules of your own that use other parameters in relation to volume quotas.

Information on the volume that users download from the web is stored on the appliance. When the configured volume quota has been exceeded for a user, a request that this user sends is blocked. A message is displayed to the user stating why the request was blocked.

Users are identified by the user names they submitted for authentication. If no user name is sent with a request, web usage is recorded and blocked or allowed for the IP address of the client system that the request was sent from.

Web downloads can be limited to volume downloaded per day, per week, or per month.

Configure volume quotas

You can configure volume quotas to limit the volume that user of your network consume during their web usage.

Task

1. Select **Policy** | **Rule Sets**.
2. On the rule sets tree, expand the rule set that contains rules for the volume quota , for example, the **Volume Quota** library rule set.

   The nested rule sets appear.
3. Select the appropriate nested rule set, for example, **Volume Quota With IP Configuration**.

   The general settings and rules of the rule set appear on the settings pane.
4. In the rule set criteria, click the appropriate blocking list name, for example, **IP Block List for Volume Quota**.

   > A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

   The **Edit List (Category)** window opens.
5. Add the appropriate entries to the blocking list, for example, IP addresses. Then click **OK** to close the window.
6. In the criteria for one of the rules, click the appropriate settings name, for example, **IP Configuration**.

   The **Edit Settings** window opens.
7. Configure the appropriate parameters, for example, session time and the volume quota per day, week, and month. Then click **OK** to close the window.
8. Click **Save Changes**.

See also

Volume Quota settings on page 178

Volume Quota settings

The Volume Quota settings are used for configuring the module that handles volume quota management.

Volume Quota per Day, Week, and Month

Settings for volume quotas

When a time unit or the session time is selected, the heading of the next section reads accordingly.

Table 9-4 Volume Quota per Day, Week, and Month

Option	Definition
Volume quota per day (week, month)	When selected, the quota that is configured in the next section applies to the selected time unit
Session time	When selected, the quota that is configured in the next section applies to the session time

Volume for . . .

Settings for volume quotas that apply to the selected time unit or the session time

The heading of this section varies according to what you selected in the preceding section.

For example, if you selected *Volume quota per week*, the heading reads *Volume for Volume Quota per Week*.

However, if you selected *Session Time*, the heading reads *Hours and Minutes*.

Table 9-5 Volume for . . .

Option	Definition
GiB	Number of GiB that are allowed as volume
MiB	Number of MiB that are allowed as volume

Actual Configured Volume Quota

Displays the configured volume quotas.

Table 9-6 Actual Configured Volume Quota

Option	Definition
Volume quota per day (week, month)	Allowed volume per day, week, or month
Session time	Allowed session time

Volume Quota rule set

The Volume Quota rule set is a library rule set for imposing volume quotas on web usage.

Library rule set – Volume Quota
Criteria – *SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to other communication that does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Time Quota With URL Configuration
- Time Quota With IP Configuration

  This nested rule set is not enabled initially.
- Time Quota With Authenticated User Configuration

  This nested rule set is not enabled initially.

Library rule set – Volume Quota
Criteria – *SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Volume Quota With URL Configuration
- Volume Quota With IP Configuration

  This rule set is not enabled initially.

- Volume Quota With Authenticated User Configuration

  This rule set is not enabled initially.

- Volume Quota With Media Type Configuration

  This rule set is not enabled initially.

Volume Quota With URL Configuration

This nested rule set handles volume quotas related to URL categories.

Nested library rule set – Volume Quota With URL Configuration
Criteria – *URL.Categories<Default> at least one in list URL Categories Blocklist for Volume Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for volume quotas related to URL categories.

The rule set contains the following rules:

Redirecting after starting new time session

Quota.Volume.IsActivationRequest<URL Category Configuration> equals true –>
Redirect<Redirection After Volume Session Activation>

The rule redirects a request to let a user again access a web object after session time has been exceeded and the user has chosen to continue with a new session.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles volume quotas.

The action settings specify a message to the requesting user.

Check if volume session has been exceeded

Quota.Volume.Session.Exceeded<URL Category Configuration> equals true –>
Block<ActionVolumeSessionBlocked>

The rule uses the *Quota.Volume.SessionExceeded* property to check whether the configured session time has been exceeded for a user. If it has, the user's request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles volume quotas.

The action settings specify a message to the requesting user.

Check if volume quota has been exceeded

Quota.Time.Exceeded<URL Category Configuration> equals true –>
Block<ActionVolumeSessionBlocked>

The rule uses the *Quota.Volume.Exceeded* property to check whether the configured volume quota has been exceeded for a user. If it has, the user's request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles volume quotas.

The action settings specify a message to the requesting user.

Volume Quota With IP Configuration

This nested rule set handles volume quotas related to IP addresses.

Nested library rule set – Volume Quota With IP Configuration
Criteria – *Client.IP is in list IP Blocklist for Volume Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for volume quotas related to IP addresses.

The rules in this rule set are the same as in the Volume Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *IP Configuration*.

Volume Quota With Authenticated User Configuration

This nested rule set handles volume quotas related to user names.

Nested library rule set – Volume Quota With Authenticated User Configuration
Criteria – *Authenticated.RawUserName is in list User Blocklist for Volume Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for volume quotas related to user names.

The rules in this rule set are the same as in the Volume Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *Authenticated User Configuration*.

Volume Quota With Media Type Configuration

This nested rule set handles volume quotas related to media types.

Nested library rule set – Volume Quota With Media Type Configuration
Criteria – *MediaType.FromFileExtension at least one n list Media Type Blocklist for Volume Quota*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is sent to access a web object belonging to a media type that is on the blocking list for volume quotas related to media types.

The rules in this rule set are the same as in the Volume Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *Media Type Configuration*.

Coaching

By configuring coaching quotas, you can limit the time that users of your network are allowed to spend for web usage, but allow them to continue if they choose to do so.

To coach the web usage of your users, you configure a coaching session with a particular length of time. When this session time has elapsed for a user, a block message is displayed. The user can then choose to start a new session.

You can configure coaching in relation to the parameters used in the Coaching library rule set, such as URL categories, IP addresses, and user names. You can also create rules of your own using other parameters.

Configure coaching

You can configure coaching to restrict web usage for the users of your network, but allow them to continue when they choose to do so after the configured time limit has been exceeded.

Task

1. Select **Policy | Rule Sets**.
2. On the rule sets tree, expand the rule set that contains rules for coaching, for example, the **Coaching** library rule set.

   The nested rule sets appear.
3. Select the appropriate nested rule set, for example, **Coaching With IP Configuration**.

   The general settings and rules of the rule set appear on the settings pane.
4. In the rule set criteria, click the appropriate blocking list name, for example, **IP Block List for Coaching**.

   A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

   The **Edit List (Category)** window opens.
5. Add the appropriate entries to the blocking list, for example, IP addresses. Then click **OK** to close the window.
6. In the criteria for one of the rules, click the appropriate settings name, for example, **IP Configuration.**

   The **Edit Settings** window opens.
7. Configure the appropriate parameters, for example, the session time. Then click **OK** to close the window.
8. Click **Save Changes**.

See also

Coaching settings on page 182

Coaching settings

The Coaching settings are used for configuring the module that handles coaching.

Hours and Minutes of Session Time

Settings for configuring the length of a coaching session

Table 9-7 Hours and Minutes of Session Time

Option	Definition
Days	Days of a coaching session
Hours	Hours of a coaching session
Minutes	Minutes of a coaching session

Coaching rule set

The Coaching rule set is a library rule set for imposing restrictions on web usage that can users can pass by if they choose to do so.

Library rule set – Coaching
Criteria – *SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Coaching With URL Configuration
- Coaching With IP Configuration

  This rule set is not enabled initially.
- Coaching With Authenticated User Configuration

  This rule set is not enabled initially.

Coaching With URL Configuration

This nested rule set handles coaching related to URL categories.

Nested library rule set – Coaching With URL Configuration
Criteria – *URL.Categories<Default> at least one in list URL Categories Blocklist for Coaching*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for coaching related to URL categories.

The rule set contains the following rules:

Redirecting after starting new coaching session

Quota.Coaching.IsActivationRequest equals true –> Redirect<Redirection After Coaching Session Activation>

The rule redirects a request to let a user again access a web object after session time has been exceeded and the user has chosen to continue with a new session.

The action settings specify a message to the requesting user.

Check if coaching session has been exceeded

Quota.Coaching.Session.Exceeded<URL Category Configuration> equals true –> Block<ActionCoachingSessionBlocked>

The rule uses the *Quota.Coaching.SessionExceeded* property to check whether the configured session time has been exceeded for a user. If it has, the user's request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles coaching.

The action settings specify a message to the requesting user.

Coaching Quota With IP Configuration

This nested rule set handles coaching related to IP addresses.

Nested library rule set – Coaching With IP Configuration
Criteria – *Client.IP is in list IP Blocklist for Coaching*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for coaching related to IP addresses.

The rules in this rule set are the same as in the Coaching with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *IP Configuration*.

Coaching With Authenticated User Configuration

This nested rule set handles coaching related to user names.

Nested library rule set – Coaching With Authenticated User Configuration
Criteria – *Authenticated.RawUserName is in list User Blocklist for Coaching*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for coaching related to user names.

The rules in this rule set are the same as in the Coaching with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are *Authenticated User Configuration*.

Authorized override

You can configure session time for a session that allows authorized overriding.

When this session time has elapsed, a user request is blocked and a block message is displayed. The message also asks for submission of a user name and password to start a new session.

These credentials must be those of an authorized user. For example, in a classroom situation, a user who gets blocked after termination of an authorized override session could be a student, while the teacher is the authorized user.

Authentication of this user is performed according to the configured authentication method. However, when configuring this method, you cannot let it include an integrated authentication mode.

The block message also provides an option to specify the time length of the authorized override session for the user who was blocked.

The time length that is configured for this user should not exceed the time length configured for all other users as part of the module settings for authorized overriding.

You can configure authorized overriding in relation to the parameters used in the library rule set, such as URL categories, IP addresses, and user names. You can also create rules of your own using other parameters.

Configure authorized overriding

You can configure authorized overriding to restrict the web usage of your users, but allow the configured time limit to be passed by through the action of an authorized user.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, expand the rule set that contains rules for authorized overriding, for example, **Authorized Override** library rule set.

The nested rule sets appear.

3 Select the appropriate nested rule set, for example, **Authorized Override With IP Configuration**.

The general settings and rules of the rule set appear on the settings pane.

4 In the rule set criteria, click the appropriate blocking list name, for example, **IP Block List for Authorized Override**.

ℹ A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

The **Edit List (Category)** window opens.

5 Add the appropriate entries to the blocking list, for example, IP addresses. Then click **OK** to close the window.

6 In the criteria for one of the rules, click the appropriate settings name, for example, **IP Configuration.**

The **Edit Settings** window opens.

7 Configure the appropriate parameters, for example, the session time. Then click **OK** to close the window.

8 Click **Save Changes**.

See also
Authorized Override settings on page 185

Authorized Override settings

The Authorized Override settings are used for configuring the module that handles authorized overriding.

Hours and Minutes of Maximum Session Time

Settings for configuring the maximum time length of a session with authorized overriding.

Table 9-8 Hours and Minutes of Maximum Session Time

Option	Definition
Days	Days of an Authorized Override session
Hours	Hours of an Authorized Override session
Minutes	Minutes of an Authorized Override session

Authorized Override rule set

The Authorized Override rule set is a library rule set for imposing a time limit on web usage that can be passed by through the action of authorized user.

Library rule set – Authorized Override
Criteria – *SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Authorized Override With URL Configuration
- Authorized Override With IP Configuration

  This rule set is not enabled initially.
- Authorized Override With Authenticated User Configuration

  This rule set is not enabled initially.

Authorized Override With URL Configuration

This nested rule set handles authorized overriding related to URL categories.

Nested library rule set – Authorized Override With URL Configuration
Criteria – *URL.Categories<Default> at least one in list URL Categories Blocklist for Authorized Override*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for authorized overriding related to URL categories.

The rule set contains the following rules:

Redirect after authenticating for authorized override

Quota.AuthorizedOverride.IsActivationRequest<URL Category Configuration> equals true AND Authentication.Authenticate<User Database> equals true –> Redirect<Redirection After Authorized Session Activation>

The rule redirects a request to let a user again access a web object after session time has been exceeded and the credentials the user submitted to continue with a new session have been validated.

The action settings specify a message to the requesting user.

Check if authorized override session has been exceeded

Quota.AuthorizedOverride.SessionExceeded<URL Category Configuration> equals true –> Block<Action Authorized Override Blocked>

The rule uses the *Quota.AuthorizedOverride.SessionExceeded* property to check whether the configured session time has been exceeded for a user. If it has, the user's request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles authorized overriding.

The action settings specify a message to the requesting user.

Authorized Override With IP Configuration

This nested rule set handles authorized overriding related to IP addresses.

Nested library rule set – Authorized Override With IP Configuration
Criteria – *Client.IP is in list IP Blocklist for Authorized Override*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for authorized overriding related to IP addresses.

The rules in this rule set are the same as in the Authorized Override with URL Configuration rule set, except for the module settings in the rule criteria, which are *IP Configuration*.

Authorized Override With Authenticated User Configuration

This nested rule set handles authorized overriding related to user names.

Nested library rule set – Authorized Override With Authenticated User Configuration
Criteria – *Authenticated.RawUserName is in list User Blocklist for Authorized Override*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for authorized overriding related to user names.

The rules in this rule set are the same as in the Authorized Override with URL Configuration rule set, except for the module settings in the rule criteria, which are *Authenticated User Configuration*.

Blocking sessions

By configuring blocking sessions you can block requests sent by a user for a configured period of time.

A blocking session is imposed after a user has sent a request that is blocked according to a configured rule, for example, a request for a URL that falls into a category that is not allowed.

This is a means of enforcing a web security policy that handles unwanted access to web objects with more strictness.

You can configure blocking sessions in relation to the parameters that are used in the library rule set. You can also create rules of your own using other parameters.

Configure blocking sessions

You can configure blocking sessions to block session for a user over a configured period of time after an attempt to access a web object that is not allowed.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, expand the rule set that contains rules for the blocking session, for example, the **Blocking Sessions** library rule set.

  The nested rule sets appear.

3 Select the appropriate nested rule set, for example, **Blocking Sessions With IP Configuration**.

  The general settings and rules of the rule set appear on the settings pane.

4 In the rule set criteria, click the appropriate blocking list name, for example, **IP Block List for Blocking Sessions**.

> A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

The **Edit List (Category)** window opens.

5 Add the appropriate entries to the blocking list, for example, IP addresses. Then click **OK** to close the window.

6 In the criteria for one of the rules, click the appropriate settings name, for example, **IP Configuration**.

The **Edit Settings** window opens.

7 Configure the appropriate parameters, for example, the period of time over which sessions are blocked. Then click **OK** to close the window.

8 Click **Save Changes**.

See also

Block Session settings on page 188

Block Session settings

The Block Session settings are used for configuring the module that handles blocking sessions.

Hours and Minutes for Session Time

Settings for configuring the time length of a blocking session

Table 9-9 Hours and Minutes for Session Time

Option	Definition
Days	Days of the blocking session
Hours	Hours of the blocking session
Minutes	Minutes of the blocking session

Blocking Sessions rule set

The Blocking Sessions rule set is a library rule set for blocking web sessions after an attempt to access a web object that is not allowed.

Library rule set – Blocking Sessions
Criteria – *SSL.Client.Context.IsApplied equals true OR Command.Name does not equal “CONNECT”*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule set is nested in this rule set: *Blocking Sessions With URL Configuration*

Blocking Sessions With URL Configuration

This nested rule set handles blocking sessions related to URL categories.

Nested library rule set – Blocking Sessions With URL Configuration
Criteria – *URL.Categories<Default> at least one in list URL Categories Blocklist for Blocking Sessions*
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for blocking sessions related to URL categories.

The rule set contains the following rules:

Block user if blocking session is active

BlockingSession.IsBlocked<Blocking Session Configuration> equals true –> Block<Blocking Session Template>

The rule uses the *BlockingSession.IsBlocked* property to check whether a blocking session has been activated for a user who sends a request. If it has, the request is blocked.

The action settings specify a message to the requesting user.

Activate blocking session if category is in list Category List for Blocking Sessions

URL.Categories<Default> at least one in list Category List for Blocking Session –> Continue — BlockingSession.Activate<Blocking Session Configuration>

The rule uses the *URL.Categories* property to check whether a URL that a user requests access to falls into a category on the blocking list maintained especially for blocking sessions. If it falls into a category on the list, a blocking session is activated for the user.

The *BlockingSession.Activate* event is used to activate the blocking session. The event settings are specified with the event.

Quota system settings

Quota system settings are general settings for time intervals related to quota management .

If an appliance is a node in a Central Management configuration, you can configure time intervals for data synchronization with other nodes.

These settings are configured on the **Appliances** tab of the **Configuration** top-level menu.

They can also appear under the name of **Coaching** (instead of Quota), but apply in both cases to all options that are provided for quota management: Authorized override, blocking sessions, coaching, time quota, and volume quota.

Quota Intervals for Synchronisation and Saving in Minutes

Settings for time intervals related to quota management

Table 9-10 Quota Intervals for Synchronisation and Saving in Minutes

Option	Definition
Save interval	Time (in minutes) to elapse before current quota values are saved on an appliance, for example, the volume in bytes that has been consumed by a particular user
Interval for sending updated quota data	Time (in minutes) to elapse before current quota values are distributed from an appliance to all nodes in a Central Management configuration The distributed data includes the changes in quota values that have occurred since the last time that data were distributed from the appliance.

Table 9-10 Quota Intervals for Synchronisation and Saving in Minutes *(continued)*

Option	Definition
Interval for base synchronisation	Time (in minutes) to elapse before quota values are synchronized on all nodes in a Central Management configuration The synchronization takes a snapshot of the current quota values on all appliances. The values that are most recent with regard to individual users are distributed to all appliances. The values are also distributed to nodes that were temporarily inactive and did not receive updates sent during that time. They are, furthermore, distributed to nodes that have been newly added to the configuration, so they did not receive any previous updates.
Cleanup database after	Time (in days) to elapse before data is deleted in the quota database Before data is deleted, a check is performed to see whether the data is obsolete. Data is obsolete if the time interval that has been configured for a quota management function has elapsed. For example, if a particular amount of bytes has been configured as volume quota for a user to be consumed during a month, the amount that the user actually consumed during a month becomes obsolete when a new month begins. The cleanup then deletes this data if the time configured under the **Cleanup database after** option has also elapsed. Stored data becomes obsolete after a month for time quotas. For other quota management functions, other time intervals are relevant. For example, for coaching and authorized overriding, the cleanup cannot be performed before the allowed session time has elapsed.

10 Web filtering

When users of your network send requests to access the web, the appliance filters these requests, as well as the responses that are sent back from the web. Embedded objects sent with requests and responses are also filtered.

Web filtering is performed in different ways. It is controlled by rules, which you can implement and modify. Default filtering on the appliance includes:

- **Virus and malware filtering** — Blocks access to web objects that are infected
- **URL filtering** — Blocks access to web objects with particular URLs
- **Media type filtering** — Blocks access to web objects that belong to particular media types

Global whitelisting allows access to web objects before any of the rules for the above filtering methods are applied. SSL scanning enables the filtering and eventual blocking of requests that are sent using SSL-secured connections.

Contents

Virus and malware filtering

Virus and malware filtering ensures that the users of your network cannot access infected web objects. The filtering process detects infections and blocks access accordingly.

The following elements are involved in this process:

- Filtering rules that control the process
- Whitelists that are used by rules to exempt particular web objects from further filtering
- The Anti-Malware module, which is called by a suitable rule to scan web objects for infections by viruses and other malware

Filtering rules

The rules that control virus and malware filtering are usually contained in one rule set. The key rule in this rule set is the one that blocks access to web objects if they are infected by viruses and other malware.

To find out whether an object is infected, the rule calls the Anti-Malware module, which scans the object and lets the rule know about the result.

Whitelisting rules can be placed and processed in this rule set before the blocking rule. If any of them applies, the blocking rule is skipped and the whitelisted objects are not scanned.

You can review the rules that are implemented on the appliance for virus and malware filtering, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for virus and malware filtering is included. Its name is *Gateway Antimalware*.

Whitelists

Whitelists are used by whitelisting rules to let the blocking rule be skipped for particular web objects, which means no scanning is applied to these objects. There can be whitelists for URLs, media types, and other types of objects.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the whitelisting rules.

Blocking lists are typically not used in virus and malware filtering because here the blocking depends not on entries in lists, but on the findings of the Anti-Malware module.

Anti-Malware module

The Anti-Malware module is also known as the Anti-Malware *engine*. It scans objects to detect infections by viruses and other malware. According to the findings of this module, the blocking rule blocks access to web objects or lets them pass through.

When the Anti-Malware module is called to run and scan web objects, it is by default a combination of two modules (engines) that are running. These modules can be seen as submodules of the Anti-Malware module.

Each of the submodules uses different scanning methods. When configuring settings for the Anti-Malware module, you can alter the default mode to have a third-party submodule running in addition or alone.

The two submodules that are running by default are the *McAfee Gateway Anti-Malware engine*, and the *McAfee Anti-Malware engine*. The latter uses virus signatures to detect infections in web objects.

However, this method can only detect viruses and other malware that are already known and have been given signatures. To ensure a higher level of web security, the McAfee Gateway Anti-Malware engine uses also proactive methods to detect new viruses and malware.

To avoid temporary overloading of the submodules, you can configure an anti-malware queue that requests are moved to before being scanned.

Configure virus and malware filtering

You can configure virus and malware filtering to adapt this process to the requirements of your network.

Complete the following high-level steps.

Task

1. Review the rules in the rule set for virus and malware filtering.

   By default, this is the *Gateway Antimalware* rule set.

2. Modify these rules as needed.

You can, for example, do the following:

- Enable or disable whitelisting rules
- Edit the lists used by the whitelisting rules

  A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

- Create whitelists of your own and let them be used by the whitelisting rules
- Modify the combination of submodules that run when the Anti-Malware module is called to scan web objects

  By default, the combination includes the following submodules:

  - McAfee Gateway Anti-Malware
  - McAfee Anti-Malware
- Modify other settings of the Anti-Malware module

3 Configure the anti-malware queues as needed to avoid overloading of the modules that scan web objects.

4 Save your changes.

Configure the Anti-Malware module

You can configure the Anti-Malware module to modify the way web objects are scanned for infections by viruses and other malware.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select the rule set for virus and malware filtering.

  By default, this is the *Gateway Antimalware* rule set.

  The rules of the rule set appear on the settings pane.

3 Make sure **Show details** is selected.

4 Find the rule that calls the Anti-Malware module.

  By default, this is the rule *Block if virus was found*.

5 In the rule criteria, click the settings name.

  This name appears next to the *Antimalware.Infected* property. By default, it is *Gateway Antimalware*.

  The **Edit Settings** window opens. It provides the settings for the Anti-Malware module.

6 Configure these settings as needed. Then click **OK** to close the window.

7 Click **Save Changes**.

See also

Anti-Malware settings on page 195

Change the module combination for scanning web objects

When configuring the settings of the Anti-Malware module, you can change the combination of submodules that run to scan web objects.

Different submodules can run under the name of *Anti-Malware* module (or engine) to perform the scanning. Which of them are available on your appliance depends on the licenses you have purchased.

Task

1 Select **Policy** | **Rule Sets**.

2 Access the Anti-Malware settings.

   a On the rule sets tree, select the rule set for virus and malware filtering.

   By default, this is the *Gateway Antimalware* rule set.

   The rules of the rule set appear on the settings pane.

   b Make sure **Show details** is selected.

   c Find the rule that calls the Anti-Malware module.

   By default, this is the rule *Block if virus was found*.

   d In the rule criteria, click the settings name.

   This name appears next to the *Antimalware.Infected* property. By default, it is *Gateway Antimalware*.

   The **Edit Settings** window opens. It provides the settings for the Anti-Malware module.

3 In the **Select scanning engines and behavior** section, select one of the following combinations of submodules:

- **Full McAfee coverage: The recommended high-performance configuration** — When selected, the McAfee Gateway Anti-Malware engine and the McAfee Anti-Malware engine are active.

  The scanning mode is then: *Proactive methods + virus signatures*

  This module combination is enabled by default.

- **Layered coverage: Full McAfee coverage plus specific Avira engine features – minor performance impact** — When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and, for some web objects, also the third-party Avira engine are active.

  The scanning mode is then: *Proactive methods + virus signatures + third-party module functions for some web objects*

- **Duplicate coverage: Full McAfee coverage and Avira engine – less performance and more false positives** — When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and the third-party Avira engine are active.

  The scanning mode is then: *Proactive methods + virus signatures + third-party module functions*

- **Avira only: Only uses Avira engine — not recommended** — When selected, only the Avira engine is active.

  The scanning mode is then: *Third-party module functions*

4 Click **OK** to close the window.

5 Click **Save Changes**.

If you select the Avira only option when working with the Gateway Antimalware rule set, you should rename the settings and the rule set to indicate that a key setting has changed.

The renaming could, for example, be from *Gateway Antimalware* (settings and rule set) to *Avira Anti-Malware* (settings and rule set).

Instead of renaming the rule set and the settings, you can also create an additional rule set and additional settings to have them available when needed for configuring rules.

Anti-Malware settings

The Anti-Malware settings are used for configuring the way the Anti-Malware module scans web objects for infections by viruses and other malware.

Select Scanning Engines and Behavior

Settings for selecting a combination of scanning engines and their behavior in case one of them detects an infection

The scanning engines are the submodules that run together as the Anti-Malware module to scan web objects

Table 10-1 Select Scanning Engines

Option	Definition
Full McAfee coverage: The recommended high-performance configuration	When selected, the McAfee Gateway Anti-Malware engine and the McAfee Anti-Malware engine are active. Web objects are then scanned using: *Proactive methods + Virus signatures* This option is selected by default.
Layered coverage: Full McAfee coverage plus specific Avira engine features — minor performance impact	When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and, for some web objects, also the third-party Avira engine are active. Web objects are then scanned using: *Proactive methods + Virus signatures + Third-party module functions for some web objects*
Duplicate coverage: Full McAfee coverage and Avira engine — less performance and more false positives	When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and the third-party Avira engine are active. Web objects are then scanned using: *Proactive methods + Virus signatures + Third-party module functions*
Avira only: Only uses Avira engine — not recommended	When selected, only the Avira engine is active. Web objects are then scanned using: *Third-party module functions*
Stop virus scanning right after an engine detected a virus	When selected, engines stop scanning a web object as soon as one of them has detected an infection by a virus or other malware.

Mobile Code Behavior

Settings for configuring a risk level in classifying mobile code

The risk level can take values from 60 to 100.

A low value means the risk in proactively scanning the behavior of mobile code and not detecting that it is malware is low because the scanning methods are applied very strictly. Mobile code will then be classified as malware even if only a few criteria of being potentially malicious have been detected.

This can lead to classifying mobile code as malware that is actually not malicious (“false positives”).

While more proactive security is achieved with a stricter setting, accuracy in determining which mobile code is really malicious will suffer. Consequently, the appliance might block web objects that you want to get through to your users.

A high value means the risk in not detecting malicious mobile code is high (more “false negatives”), but more accuracy is achieved in classifiying mobile code correctly as malicious or not (fewer “false positives”).

Table 10-2 Mobile Code Behavior

Option	Definition
Classification threshold	Slider scale for setting a risk level as described above • Minimum value (maximum proactivity): 60 • Maximum value (maximum accuracy): 100

Advanced Settings

Advanced settings for all scanning submodules

Table 10-3 Advanced Settings

Option	Definition
Enable Antivirus PreScan	When selected, performance of the submodules is improved by reducing the load sent to them for scanning. This option is by default selected. We recommend not to change this setting.
Enable GTI file reputation queries	When selected, information on the reputation of files retrieved from the Global Threat Intelligence system is included in the scanning result that the Anti-Malware module provides.
Enable heuristic scanning	When selected, heuristic scanning methods are applied to web objects.

Advanced Settings for McAfee Gateway Anti-Malware

Advanced settings for the McAfee Gateway Anti-Malware submodule

The following options are by default selected. We recommend not to change these settings.

Table 10-4 Advanced Settings for McAfee Web Gateway Anti-Malware

Option	Definition
Enable detection for potentially unwanted programs	When selected, web objects are also scanned for potentially unwanted programs.
Enable mobile code scanning	When selected, mobile code is scanned in general. Individual settings can be configured under *Scan the following mobile code types*.
Enable removal of disinfectable content detected in HTML documents by mobile code filter	When selected, the content described here can be removed.
Scan the following mobile code types	
When the following mobile code types are selected, they are scanned.	

Table 10-4 Advanced Settings for McAfee Web Gateway Anti-Malware *(continued)*

Option	Definition
Windows executables	Once downloaded from the web or received by email, these executables can become a threat when launched because they run with all the privileges of the current user.
JavaScript	JavaScript code can be embedded virtually anywhere, from web pages and PDF documents to video and HTML files.
Flash ActionScript	ActionScript code can be embedded in flash videos and animations and has access to the flash player and the browser with all their functions.
Java applets	Java applets can be embedded in web pages. Once activated, they can run at different permission levels, based on a digital certificate and the user's choice.
Java applications	Java applications run stand-alone with all privileges of the current user.
ActiveX controls	ActiveX controls can be embedded in web pages and office documents. Once activated, they run with all privileges of the current user.
Windows libraries	These libraries usually come along with an executable in a setup package or are downloaded from the web by a running executable or by malicious code.
Visual Basic script	Visual Basic script code can be embedded in web pages or in emails.
Visual Basic for applications	Visual Basic macros can be embedded in office documents created with Word, Excel, or PowerPoint.
Block the following behavior	
When the following types of behavior are selected, web objects showing this behavior are blocked.	
Data theft: Backdoor	Malicious applications that grant an attacker full remote access and control to a victim's system through existing or newly created network channels
Data theft: Keylogger	Malicious applications that hook into the operating system to record and save keyboard strokes The captured information, such as passwords, is sent back to the attacking party.
Data theft: Password stealer	Malicious applications that gather, store, and leak sensitive information, such as the system configuration, confidential data, credentials, and other data for user authentication
System compromise: Code execution exploit	Exploits for vulnerabilities in any client applications, such as browsers, office programs, or multi-media players, that could allow an attacker to run arbitrary code on the compromised system
System compromise: Browser exploit	Exploits for vulnerabilities in browser applications and plug-ins that could allow the attacker to run arbitrary code, steal sensitive data, or escalate privileges
System compromise: Trojan	Malicious applications that pretend to be harmless or useful, but actually perform malicious activities

Table 10-4 Advanced Settings for McAfee Web Gateway Anti-Malware *(continued)*

Option	Definition
Stealth activity: Rootkit	Malicious applications or device drivers that manipulate the operating system and hide presence of malware on infected systems After the compromise, files, registry keys, and network connections belonging to the malware processes turn invisible and could be hard to recover.
Viral Replication: Network worm	Malicious applications or device drivers that self-replicate using email, the internet, peer-to-peer networking, or by copying themselves onto removable media such as USB devices
Viral Replication: File infector virus	Self-replicating applications that infect existing files on the hard-disk, embedding viral code in order to spread through the newly infected host file
System compromise: Trojan downloader	Malicious applications or script code that download and execute additional payload from the internet
System compromise: Trojan dropper	Malicious applications that carry hidden payload, extract and launch it upon execution
System compromise: Trojan proxy	Malicious applications that allow to relay potentially malicious hidden network activity through the compromised system
Web threats: Infected website	Websites that contain injected malicious script code or request additional malicious code as soon as it is opened in a browser The initial infection might have taken place through an SQL injection attack against the web server.
Stealth activity: Code injection	Applications that copy their code into other, often legitimate processes, resulting in a hijacking of the respective privileges and trust This technique is typically employed by malware that tries to hide its presence on compromised systems and tries to evade detection.
Detection evasion: Obfuscated code	Applications that consist of highly scrambled of encrypted code
Detection evasion: Packed code	Applications whose content has been compressed by a run-time packer or protector Applying a run-time packer to an application changes the way it looks so it is harder to it is harder to classify.
Potentially unwanted: Ad-/Spyware	Applications that show potentially annoying or unwanted advertisements, but also track and analyze the user’s activities and behavior
Potentially unwanted: Adware	Applications that show potentially annoying or unwanted advertisements, but also track and analyze the user’s activities and behavior
Data theft: Spyware	Applications that track and analyze the user’s activities and behavior, steal sensitive data, and leak this data to the attacker’s servers
Potentially unwanted: Dialer	Applications that provide access to content, such as pornography, through a more expensive network connection
Web threats: Vulnerable ActiveX controls	Potentially vulnerable ActiveX controls that are restricted to other on-browser usage and should not be used on a web page
Potentially unwanted: Suspicious activity	Potentially malicious code that is identified by either non-standard or not fully trusted behavior
Web threats: Cross-site scripting	Malicious scripts that try to exploit browser or web application access-control vulnerabilities in browsers or web applications to steal user-specific data, such as cookies

Table 10-4 Advanced Settings for McAfee Web Gateway Anti-Malware *(continued)*

Option	Definition
Potentially unwanted: Deceptive behavior	Misleading messages, missing code tricks, and fake alerts presented to users These threats might tell users that their systems are infected with spyware and promote so-called fake AV applications for cleaning.
Potentially unwanted: Redirector	Redirecting code that forwards users visiting a website to other, potentially malicious locations This behavior is often caused by an infection of a previously legitimate website.
Potentially unwanted: Direct kernel communication	Applications that directly communicate with the Windows kernel or in kernel mode These might try to install a rootkit or to destabilize the system.
Potentially unwanted: Privacy violation	Potentially malicious code that accesses sensitive or private data This could result in eavesdropping your clipboard content or reading registry keys.
Network behavior and DLP	
Settings for handling unknown browsers, unwanted programs, and data leakage	
Forbid unknown browsers to download executables	When selected, requests for downloading executables submitted by unknown browsers are blocked.
Block requests sent by PUPs	When selected, requests sent by potentially unwanted programs (PUPs) are blocked. • **Treat as request sent by a PUP if probability is at least** — Slider scale to set the probability (in percent) for classifying a request as being sent by a potentially unwanted program
Detect unsolicited POSTs	When selected, unsolicited POST requests, which could enable data leakage, are detected.

Anti-malware queue

To avoid overloading of the modules that scan web objects for infections by viruses and other malware, requests for access to web objects are moved to a queue before being processed.

This queue is known as the *anti-malware queue*. However, moving requests to this queue will only be a solution to avoid load peaks occurring over a short period of time. Permanent overloading needs to be addressed by other measures.

When a request has been received on the appliance, it is moved to the queue by a working thread of the proxy module. It will remain there until it is fetched by another thread and forwarded to a thread of one of the scanning modules. The same applies to responses received from web servers that requests have been forwarded to.

The working threads that deliver requests and responses to the scanning modules, as well as those that belong to the scanning modules, are known as anti-malware working threads.

When configuring the anti-malware queue, you can specify the number of anti-malware working threads that are available, the size of the anti-malware queue, and the maximum time for requests and responses to stay in the queue.

Configure the anti-malware queue

You can configure settings for the anti-malware queue to avoid overloading of the scanning modules.

Task

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to configure the anti-malware queue on and click **Anti-Malware**.

   The settings for the anti-malware queue appear on the settings pane.
3. Configure these settings as needed.
4. Click **Save Changes**.

Anti-Malware system settings

The Anti-Malware system settings are used for configuring the anti-malware queue.

Global Anti-Malware Settings

Settings for the anti-malware queue

Table 10-5 Global Anti-Malware Settings

Option	Definition
Number of threads for AV scanning	Number of anti-malware working threads that are available on an appliance The number you specify here applies to both the threads that forward requests and responses to threads of the scanning modules and the scanning module threads themselves. For example, if you specify 25, there will be 25 threads for forwarding and 25 for scanning.
Maximum number of jobs in the queue	Maximum number of requests or responses that can be moved to the anti-malware queue to become jobs for the scanning modules
Number of seconds a scanning job stays in the queue before being removed	Maximum time (in seconds) to elapse before a request or response is removed from the anti-malware queue if it has not been forwarded for scanning

Gateway Antimalware rule set

The Gateway Antimalware rule set is the default rule set for virus and malware filtering.

Default rule set – Gateway Antimalware
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The rule set contains the following rules.

Remove partial content for HTTP requests

Cycle.TopName equals "Request" AND (Connection.Protocol equals "http" OR Connection.Protocol equals "https") –> Continue – Header.RemoveAll ("Range")

The rule uses the *Cycle.TopName* and *Connection.Protocol* properties to check whether the current processing cycle is the request cycle and whether a request is sent in HTTP or HTTPS mode.

If this is the case, the *Header.RemoveAll* event modifies the request by removing the specification that only partial content is requested. A request for complete content is then forwarded to the relevant web server and eventually received from there, so that the complete content of a web object can be processed on the appliance.

For example, a complete archive can be opened and scanned for viruses and other malware. Malicious content that is distributed over several parts of a file can be detected by scanning the complete file, while it could go unnoticed if only parts of the file were scanned.

The Continue action lets processing continue with the next rule.

Default rule set – Gateway Antimalware
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

Block partial content for FTP requests

Cycle.TopName equals "Request" AND Connection.Protocol equals "ftp" AND Command.Categories contains "Partial" –> Block<Partial Content Not Allowed>

The rule uses the *Cycle.TopName*, *Connection.Protocol*, and *Command.Categories* properties to check whether the current processing cycle is the request cycle, the request is sent in FTP mode, and the command category used for the FTP transfer contains *Partial* as a string.

This allows the appliance to detect an FTP request for partial content and block it.

Unlike with HTTP or HTTPS requests, an FTP request for partial content cannot be modified to make it a request for complete content. However, security problems would arise if partial content was accepted on the appliance, which are the same as the ones that were explained in the comment on the rule for blocking HTTP and HTTPS requests.

The action settings specify a message to the requesting user.

Allow if user agent matches User Agent Whitelist

Header.Request.Get ("User-Agent") matches in list User Agent WhiteList –> Stop Rule Set

The rule uses the *Header.Request.Get* property to check the user agent information that is sent with the header of a request.

If the user agent in question is on the specified whitelist, processing of the rule set stops, so the blocking rule at the end of the rule set is not processed.

A parameter of the property specifies that it is the user agent information that must be checked when the rule is processed.

This rule is not enabled by default.

> ℹ Using this rule alone for whitelisting will cause a security problem because usually a client can set whatever user agent it prefers.

Allow URL hosts that match in list Antimalware URL Whitelist

URL.Host matches in list Antimalware URL Whitelist –> Stop Rule Set

The rule uses the *URL.Host* property to check whether a given URL matches one of the entries on the specified whitelist.

If it does, processing of the rule set stops and the blocking rule at the end of the rule set is not processed.

You can use this rule to exempt web traffic from filtering when the hosts of the URLs involved are well-known web servers for which it is safe to assume that they spread no viruses and other malware.

Whitelisting increases performance because it avoids the effort of scanning the respective web objects.

Allow streaming media from list Antimalware Media Whitelist

(URL Categories<Default> contains Streaming Media OR

URL Categories<Default> contains Internet Radio / TV OR

URL Categories<Default> contains General News)

AND MediaType.Ensured all in list Antimalware Media Type Whitelist –> Stop Rule Set

The rule uses the *URL.Categories* property to check whether a given URL belongs to Streaming Media or related categories.

When the URL Filter module is called to retrieve category information, it runs with the *Default* settings, as specified with the property.

The second part of the criteria uses the *MediaType.Ensured* property to check if the media type of a web object is found on the specified whitelist.

If the URL belongs to one of the categories in question, and the web object that is located by the URL is of a media type on the whitelist, processing of the rule set stops and the blocking rule at the end of the rule set is not processed.

The Anti-Malware module scans complete files, which means it waits for the end of data transmission before starting the scan. As streaming media is by nature an endless stream of data, the Anti-Malware module would wait forever.

However, the risk that streaming media will contain a virus or other malware is very low. Therefore, streaming media can be exempted from scanning.

Block if virus was found

Antimalware.Infected<Gateway Antimalware> equals true –> Block<Virus Found> – Statistics.Counter.Increment (“BlockedByAntiMalware”,1)<Default>

The rule uses the *Antimalware.Infected* property to check whether a given web object is infected by a virus or other malware.

When the Anti-Malware module is called to scan the object, it runs with the Gateway Antimalware settings, as specified with the property. These settings let the module use all its three submodules and their methods to scan web objects.

If the module finds that a web object is infected, processing of all rules stops and the object is not passed on further. Access to it is blocked this way.

In a request cycle, the infected web object is not passed on to the web. In the response and embedded object cycles, it is not passed on to the user who requested it.

The action settings specify a message to this user.

The rule also uses an event to count blocking due to virus and malware infections.

The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

URL filtering

URL filtering ensures that the users of your network cannot access web objects when their URLs are not allowed. The filtering process uses category information and reputation scores and blocks access accordingly.

The following elements are involved in this process:

- Filtering rules that control the process
- A whitelist and blocking lists that are used by rules to exempt some URLs from filtering and block others
- The URL filter module, which is called by suitable rules to retrieve information on URL categories and web reputation scores from the Global Threat Intelligence system

Filtering rules

The rules that control the URL filtering process are contained in a URL filtering rule set. One of these rules says, for example, that access to a URL is blocked if it matches an entry on a blocking list.

Another rule blocks URLs if they belong to a category that is on a blocking list. This rule calls the URL filter module to retrieve category information for URLs from the Global Threat Intelligence system. Another rule works in a similar way to block URLs that have a bad reputation.

A whitelisting rule exempts URLs from filtering if they match entries on the list used by the rule. This rule is placed and processed before the blocking rules. If it applies, the blocking rules are skipped and no URL filtering is performed for the whitelisted objects.

You can review these rules, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for virus and malware filtering is included. Its name is *URL Filtering*.

Whitelist and blocking lists

A whitelist is used by a whitelisting rule to let particular URLs skip the blocking rule, which means there is no URL filtering for these objects.

Another rule blocks URLs if they belong to a category that is on a blocking list. This rule calls the URL filter module to retrieve category information for URLs from the Global Threat Intelligence system. Another rule works in a similar way to block URLs that have a bad reputation.

Since a URL filtering rule set handles only URL filtering, whitelists are not needed for several types of objects as they are in virus and malware filtering.

Blocking lists are used by rules for blocking URLs according to the categories they belong to or because they match an entry on a list. Each of the blocking rules uses its own list.

Filter module

The URL filter module (also known as *engine*) retrieves information on URL categories and reputation scores from the Global Threat Intelligence™ system that is maintained by McAfee. Based on this information, blocking rules block access to URLs.

Various technologies, such as link crawlers, security forensics, honeypot networks, sophisticated auto-rating tools, and customer logs are used to gather this information. An international, multi-lingual team of McAfee web analysts evaluates the information and enters URLs under particular categories into a database.

To gather information on the reputation of a URL, its behavior on a worldwide real-time basis is analyzed, for example, where a URL shows up in the web, its domain behavior, and other details.

You can configure settings for this module, for example, to let it include category information retrieved from an extended list that you provide or to perform a DNS lookup for URLs and include the corresponding IP address in the search for category information.

Configure URL filtering

You can configure URL filtering to adapt this process to the needs of your network.

Complete the following high-level steps.

Task

1. Review the rules in the rule set for URL filtering.

   By default, this is the *URL Filtering* rule set.

2. Modify these rules as needed.

   You can, for example, do the following.

   - Enable or disable blocking rules and the whitelist rule
   - Edit the lists used by these rules

     ℹ A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

   - Modify the settings of the URL Filter module

3. Save your changes.

Configure the URL Filter module

You can configure the URL Filter module to modify the way information on URL categories and reputation scores is retrieved from the Global Threat Intelligence system.

Task

1. Select **Policy** | **Rule Sets**.

2. On the rule sets tree, select a rule set for URL filtering.

   In the default rule set system, rule sets for URL filtering are nested in the rule sets for content filtering.

   The rules appear on the settings pane.

3. Make sure **Show details** is selected.

4. Find the rule that uses a category blocking list.

   By default, this is the rule *Block URLs whose category is in Category BlockList*.

5. In the rule criteria, click the settings name.

   This name appears next to the *URL.Categories* property. By default, it is *Default*.

   The **Edit Settings** window opens. It provides the settings for the URL Filter module.

6. Configure these settings as needed.

7. Click **OK** to close the window.

8. Click **Save Changes**.

See also

URL Filter settings on page 205

URL Filter settings

The URL Filter settings are used for configuring the way the URL Filter module retrieves information from the Global Threat Intelligence system.

Extended List

Settings for extended lists

Table 10-6 Extended List

Option	Definition
Use the extended list	List for selecting an extended list
Add	Opens the **Add List** window for adding an extended list.
Edit	Opens the **Edit List (Extended List)** window for editing the selected extended list.

Rating Settings

Settings for retrieving rating information on URLs based on categories and reputation scores

Table 10-7 Rating Settings

Option	Definition
Search the CGI parameters for rating	When selected, CGI parameters are included in the search for information. CGI (Common Gateway Interface) parameters in a URL trigger scripts or programs when the URL is accessed. Information on CGIs can affect the categorization of a URL.
Search for and rate embedded URLs	When selected, embedded URLs are included in the search for information and rated. Information on an embedded URL can affect the categorization of the embedding URL. ℹ Searching for embedded URLs can impact performance.
Do a forward DNS lookup to rate URLs	When selected, a DNS lookup is performed for a URL that no relevant information has been found for. The IP address that was looked up is used for another search.
Do a backward DNS lookup for unrated IP-based URLs	When selected, a backward DNS lookup, based on its IP address, is performed for a URL that no relevant information has been found for. The host name that was looked up is used for another search.
Use the built-in keyword list	When selected, the built-in keyword list is included in the search.
Only use online GTI web reputation and categorization services	When selected, information on URL categories and reputation scores is only retrieved from the Global Threat Intelligence system.

Table 10-7 Rating Settings *(continued)*

Option	Definition
Use online GTI web reputation and categorization services if local rating yields no results	When selected, information on URL categories and reputation scores is only retrieved from the Global Threat Intelligence system if the search in the internal database yielded no results.
Use default GTI server for web reputation and categorization services	When selected, the appliance connects to the default server for retrieving information on URL categories and reputation scores from the Global Threat Intelligence system. • **IP of the server** — IP address of the server used to connect to the Global Threat Intelligence system when the default server is not used Format: <domain name> or <IPv4 address> or <IPv4 address mapped to IPv6 address> Regular IPv6 addresses cannot be specified here. • **Port of the server** — Port number of the port on this server that listens to requests from the appliance Allowed range: 1–65535

Advanced Settings

Advanced settings for the URL Filter module

Table 10-8 Advanced Settings

Option	Definition
Treat connection problems to the cloud as errors	When selected, problems arising on the connection from the appliance to the Global Threat Intelligence server are logged as errors. Properties for error handling are set and eventually rules from an Error Handler rule set are executed.
Do a backward DNS lookup also for private addresses	When selected, private IP addresses are included in the backward DNS lookup. Excluding these addresses from the lookup leads to an increase in performance for URL filtering. This option is disabled by default. The lookup includes the following types of addresses: • IPv4 • Private addresses • Zeroconf addresses • IPv6 • Link local addresses • Site local addresses • Unique local addresses

Settings for configuring a proxy the appliance can use to connect to the Global Threat Intelligence™ system

Table 10-9 Proxy Settings

Option	Definition
Use upstream proxy	When selected, the appliance uses a proxy for connecting to the Global Threat Intelligence server on which lookups for URL category information, also known as "in-the-cloud" lookups, can be performed.
IP or name of the proxy	IP address or host name of the proxy

Table 10-9 Proxy Settings *(continued)*

Option	Definition
Port of the proxy	Number of the port on the proxy that listens for lookup requests from the appliance
User name	User name for the appliance when logging on to the proxy
Password	Password for the appliance
Set	Opens a window for setting the password.

Settings for logging URL filtering activities on the appliance

Table 10-10 Logging

Option	Definition
Enable logging	When selected, URL filtering activities are logged on the appliance. If this option is not selected, the following logging options are grayed out.
Log level	List for selecting the log level: Log levels are as follows: • 00 FATAL — Logs only fatal errors • 01 ERRORS — Logs all errors • 02 WARNING — Logs errors and warnings • 03 INFO — Logs errors, warnings, and additional information • 04 DEBUG1 ... 013 DEBUG9 — Log information required for debugging URL filtering activities The amount of logged information increases from level DEBUG1 to DEBUG9. • 14 TRACE — Logs information required for tracing URL filtering activities • 15 ALL — Logs all URL filtering activities
(Log area)	Settings for including different areas of URL filtering activities into the logging • LOG_AREA_ALL — When selected, all URL filtering activities are logged • LOG_AREA_NETWORK — When selected, activities regarding the network connections used for URL filtering are logged • LOG_AREA_DATABASE_SEARCH — When selected, activities regarding the retrieval of data for URL filtering from the internal database are logged • LOG_AREA_DNS — When selected, activities regarding a DNS lookup that is performed for URL filtering are logged • LOG_AREA_URL — When selected, activities for handling URLs, such as parsing them, are logged • LOG_AREA_CLOUD — When selected, activities regarding the retrieval of information from the Global Threat Intelligence system are logged

URL Filtering rule set

The URL Filtering rule set is the default rule set for URL filtering.

Default rule set – URL Filtering
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The rule set contains the following rules.

Allow URLs that match in URL WhiteList

URL matches in list URLWhiteList –> Stop Rule Set

The rule uses the *URL* property to check whether a given URL is on the specified whitelist. If it is, processing of the rule set stops and the blocking rules that follow the whitelisting rule are not processed.

You can use this rule to exempt URLs from filtering to make sure they are available to the users of your network and do not get blocked by any of the following blocking rules. Whitelisting also increases performance because it avoids the effort of retrieving information about the respective URLs.

Block URLs that match in URL BlockList

URL matches in list URL BlockList –> Block<URLBlocked> –> Statistics.Counter.Increment (“BlockedByURLFilter”,1)<Default>

The rules uses the *URL* property to check whether a given URL is on the specified blocking list. If it is, processing of all rules stops and the request for access to the URL is not passed on to the appropriate web server. Access to it is blocked this way.

The action settings specify a message to the requesting user.

The rule also uses an event to count blocking due to virus and malware infections. The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

Enable SafeSearchEnforcer

Always –> Continue — Enable SafeSearchEnforcer<Default>

The rule enables the SafeSearchEnforcer, which is an additional module for filtering access to web sites with adult content.

The enabling is done by executing an event. The settings of the module are specified with the event.

Processing continues with the next rule.

Allow uncategorized URLs

List.OfCategory.IsEmpty(URL.Categories<Default>) equals true –> Stop Rule Set

The rule uses the *List.OfCategory.IsEmpty* property, which has the URL.Categories property as a parameter, to check whether the list of categories for categorizing a URL is empty. This would mean that the URL is uncategorized, as it could not be assigned to any of the existing categories. Specifying the URL.Categories property as a parameter ensures that it is a particular list of categories that is checked. It is the list that is the value of this property.

To provide a list of categories as the value for the URL.Categories property, the URL Filter module is called, which retrieves this list from the Global Threat Intelligence system. The module runs with the specified Default settings.

If a URL is uncategorized, processing of the rule set stops and the blocking rules that follow this rule are not processed. The request for the URL is forwarded to the appropriate web server and, unless access to the URL is blocked in the response or embedded object cycle, the user is allowed to access the web object that was requested by submitting the URL.

Block URLs whose category is in URL Category BlockList

URL.Categories<Default> at least one in list Category BlockList –> Block<URLBlocked> — Statistics.Counter.Increment (“BlockedByURLFilter”,1)<Default>

The rule uses the *URL.Categories* property to check whether one of the categories a given URL belongs to is on the specified blocking list. The URL Filter module, which is called to retrieve information on these categories, runs with the Default settings, as specified with the property.

If one of the URL’s categories is on the list, processing of all rules stops and the request for access to the URL is not passed on to the appropriate web server. Access to it is blocked this way.

The *URLBlocked* action settings specify that the user who requested this access is notified of the blocking.

The rule also uses an event to count blocking due to URL filtering in the same way as the blocking rule for individual URLs in this rule set.

Block URLs with bad reputation

URL.IsHighRisk<Default> equals true –> Block<URLBlocked> — Statistics.Counter.Increment (“BlockedByURLFilter”,1)<default>

The rules uses the *URL.IsHighRisk* property to find out whether a URL has a reputation that lets access to it appear as a high risk. If the value for this property is true, processing of all rules stops and the request for access to the URL is not passed on to the appropriate web server. Access to it is blocked this way.

The reputation score is retrieved by the URL Filter module, which runs with the settings specified after the property.

The *URLBlocked* action settings specify that the user who requested this access is notified of the blocking.

The rule also uses an event to count blocking due to URL filtering in the same way as the blocking rule for individual URLs in this rule set.

Media type filtering

Media type filtering ensures that the users of your network cannot access media that belong to particular types, such as images, audio, or streaming media, if you block these types.

This way you can, for example, prevent your users from consuming too many resources.

The following elements are involved in the filtering process:

- Filtering rules that control the process
- Blocking lists used by rules to block access to media that belong to particular types.

Filtering rules

The rules that control virus and malware filtering are usually contained in one rule set. The key rule in this rule set is the one that blocks access to web objects if they are infected by viruses and other malware.

To find out whether an object is infected, the rule calls the Anti-Malware module, which scans the object and lets the rule know about the result.

Whitelisting rules can be placed and processed in this rule set before the blocking rule. If any of them applies, the blocking rule is skipped and the whitelisted objects are not scanned.

You can review the rules that are implemented on the appliance for virus and malware filtering, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for virus and malware filtering is included. Its name is *Gateway Antimalware*.

Blocking lists

Whitelists are used by whitelisting rules to let the blocking rule be skipped for particular web objects, which means no scanning is applied to these objects. There can be whitelists for URLs, media types, and other types of objects.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the whitelisting rules.

Blocking lists are typically not used in virus and malware filtering because here the blocking depends not on entries in lists, but on the findings of the Anti-Malware module.

Configure media type filtering

You can configure media type filtering to adapt this process to the needs of your network.

Complete the following high-level steps.

Task

1. Review the rules in the rule set for media type filtering.

   By default, this is the *Media Type Filtering* rule set.

2. Modify these rules as needed.

   You can, for example, do the following:

   - Enable or disable blocking rules
   - Edit the lists used by the blocking rules

     ℹ A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

   - Create block lists of your own and let them be used by the blocking rules

3. Save your changes.

Properties for media type filtering

Most media type filtering rules in the default rule set use the *MediaType.EnsuredTypes* property in their criteria. Using other properties lets media type filtering be executed in a different way.

There is, for example, the *MediaType.NotEnsuredTypes* property. If you use this property in the criteria of a blocking rule, the rule blocks media whose types are on a block list even if the probability that they actually are of this type is less than 50%.

You could use this property to make sure a media type gets blocked under all circumstances.

The following table lists the properties that are available for rules in media type filtering.

Table 10-11 Media type filtering properties

Property	Description
MediaType.EnsuredTypes	Property of media that have their types ensured with a probability of more than 50% This level of probability is assumed if a media type signature from an internal list on the appliance can be found in the object code of the media.
MediaType.NotEnsuredTypes	Property of media for which the probability that they actually are of their respective types is less than 50%
MediaType.FromFileExtension	Property of media for which types are assumed based on the extensions of the media type file names Extensions and the media types associated with them are looked up in an internal catalog on the appliance. There are, however, extensions that are used by more than one media type.
MediaType.FromHeader	Property of media for which types are assumed according to the content type field of the headers sent with the media Headers are read and evaluated in a standardized format. To filter headers in their original formats, you can use the Header.Get property.
MediaType.IsSupported	Property of embedded or archived media that can be extracted by the opener module of the appliance.
List.OfMediaType.IsEmpty	Property of media with types that are not on an internal list

Modify a media type filtering rule

You can modify a media type filtering rule to filter a different kind of media types by changing the property in the rule criteria. Then you also need to create a new filter list for use by the modified rule.

Tasks

- *Create a filter list for a modified rule* on page 211
  You can create a new filter list for use in a modified media type filtering rule.
- *Replace a property in a media type filtering rule* on page 211
  You can replace the property in the criteria of a media type filtering rule with a different property to let the rule filter a different kind of media types.

Create a filter list for a modified rule

You can create a new filter list for use in a modified media type filtering rule.

Task

1 Select **Policy** | **Lists**.

2 On the **Custom Lists** branch of the lists tree, select **Media Type** and click **Add**.

The **Add List** window opens.

3 In the **Name** field, type a name for the new list, for example, `Not Ensured Download Media Type Blocklist`.

4 [Optional] In the **Comment** field, type a plain-text comment on the new list.

5 [Optional] Click the **Permissions** tab and configure who is allowed to access the list.

6 Click **OK**.

The **Add List** window closes and the new list appears on the lists tree under **MediaType**.

You can now fill the entries for the new list to let the media type filtering rule know what to block or allow.

Replace a property in a media type filtering rule

You can replace the property in the criteria of a media type filtering rule with a different property to let the rule filter a different kind of media types.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select a rule set for media type filtering, for example, the nested **Download Media Type** rule set in the **Media Type Filtering** rule set.

3 Select a rule, for example, **Block types from Download Media Type Blocklist**, and click **Edit**.

The **Edit Rule** window opens with the **Name** step selected.

4 Click **Rule Criteria** and under **Criteria** select the rule. Then click **Edit**.

The **Edit Criteria** window opens.

5 Edit the rule criteria as follows:

   a From the list of properties in the left column, select a new property, for example, **MediaType.NotEnsuredTypes** (instead of *MediaType.EnsuredTypes*).

   b From the list of operands in the right column, select **Not Ensured Download Media Type Blocklist**.

6 Click **OK**.

   The window closes and the modified criteria appears under **Rule Criteria**.

7 Click **Finish**.

   The **Edit Rule** window closes and the modified rule appears within the nested rule set that you selected..

8 Click **Save Changes**.

See also
Properties for media type filtering on page 210

Media Type Filtering rule set

The Media Type Filtering rule set is the default rule set for media type filtering.

Library rule set – Media Type Filtering
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The following rule sets are nested in this rule set:

- Upload Media Type

  This rule set is not enabled by default.

- Download Media Type

Upload Media Type

This nested rule set blocks the upload of media belonging to particular media types. It is processed in request cycles when users request to upload media to the web, as well as in embedded object cycles when objects are embedded in media.

Nested library rule set – Upload Media Type
Criteria – *Always*
Cycles – Requests (and IM) and embedded objects

The rule set contains the following rule:

Block types from list Upload Media Type Blocklist

Media.TypeEnsuredTypes at least one in list Upload Media Type Blocklist –> Block<Media Type (Block List)> — Statistics.Counter.Increment (“BlockedByMediaFilter”, 1)<Default>

The rule uses the *Media.TypeEnsuredTypes* property to check for media that have their type ensured if they are on the specified list. If they are, access to the media type is blocked and processing rules stops.

The rule uses an event to count blocking due to media type filtering. The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

Processing continues with the next request that is received on the appliance.

Download Media Type

This nested rule set blocks the download of media belonging to particular media types. It is processed in response cycles when web servers send media in response to user requests for downloading them, as well as in embedded object cycles when objects are embedded in media.

Nested library rule set – Download Media Type
Criteria – *Always*
Cycles – Responses and embedded objects

The rule set contains the following rule.

Block types from list Download Media Type Blocklist

Media.TypeEnsuredTypes at least one in list Download Media Type Blocklist –> Block<Media Type (Block List)> — Statistics.Counter.Increment (“BlockedByMediaFilter”, 1)<Default>

The rule uses the *Media.TypeEnsuredTypes* property to check for media that have their type ensured if they are on the specified list. If they are, access to the media type is blocked and processing rules stops.

The rule uses an event to count blocking due to media type filtering. The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

Processing continues with the next request that is received on the appliance.

Application filtering

Application filtering ensures that the users of your network cannot access unwanted applications, which could be, for example, Facebook, Xing, and others. The filtering process checks application names and reputation scores and blocks access accordingly.

The following elements are involved in this process:

- Filtering rules that control the process
- Application lists that are used by rules to block applications
- An application system list that is updated in intervals

Information on particular applications is provided in a system list on the user interface. You can create a blocking rule for applications based on this information, which blocks access to applications using application names or risk evaluation as its criteria.

Update status and statistics of the filtering process are shown on the dashboard.

Rules for application filtering

The rules that control application filtering are usually contained in one rule set. They block access to applications using the following two methods:

- Block applications that are on a list
- Block applications that are assigned a particular risk level

To block applications according to a list, the *Application.Name* property is used.

The value of this property is the name of an application that appears in a request sent by a user who wants to access the application. If this name is on a blocking list, access is blocked, as, for example, the following rule does it.

Name

Block applications according to list

Criteria		Action
Application.Name is in list Unwanted Applications	–>	Block<Application Blocked>

To block applications according to their risk levels, properties, such as *Application.IsMediumRisk* or *Application.IsHighRisk* are used, which have *true* or *false* as their values.

Risk evaluation is based on the reputation score for an application that is assigned to it by the Global Threat Intelligence system. If the risk for allowing access to an application is considered to be high, it means it has a bad reputation.

If an application reaches or exceeds this level, access to it is blocked, as, for example, the following rule does it.

Name

Block high-risk applications

Criteria		Action
Application.IsMediumRisk equals true OR Application.isHighRisk equals true	–>	Block<Application Blocked>

Both methods rely on the application system list. Only applications that are on the system list can also appear on the lists that are used by individual rules.

Also the risk levels for applications are those that are shown on the application system list.

For logging purposes, there are also the *Application.To String* and *Application.Reputation* properties, which are the name of a requested application converted into a string and a numerical value for its reputation score, respectively.

You can use these properties in rules that record information in log file entries.

Application filtering is not perfomed by default on an appliance. However, you can import the *Application Control* rule set from the library.

You can then review the rules in this rule set, modify or delete them, and also create your own rules.

Lists for blocking applications

Blocking lists are used by rules to block access to applications that are requested by users. The rules in the library rule set include rules that are already filled with several application names.

You can add application names to a list from the library rule set or remove them and also create your own lists. If you add application names, you take them from the application system list.

Application system list

The applications that can be blocked through application filtering appear on a list, which is provided by the appliance system and updated in intervals.

You can view this list under *System Lists* on the lists tree of the *Lists* tab. For each application, it provides the following information:

- Application name
- Reputation score
- Plain-text description

Application filtering information on the dashboard

The dashboard provides the following information on application filtering:

- Update status of the application list
- Statistics on the applications that have actually been blocked

Configure application filtering

You can configure application filtering to adapt this process to the needs of your network.

Complete the following high-level steps.

Task

1. Import the *Application Control* rule set.
2. Review the rules in this rule set and modify them as needed.

   You can, for example, do the following.

   - Enable or disable blocking rules
   - Edit the lists used in rules by adding or removing applications
   - Change the reputation levels used in rules by replacing the relevant properties, for example, by replacing *Application.IsHighRisk* with *Application.IsMediumRisk*

   You can also create blocking rules of your own.
3. Save your changes.

Application Control rule set

The Application Control rule set is a library rule set for application filtering.

Library rule set – Application Control
Criteria – *Always*
Cycles – Requests (and IM), responses

The following rule sets are nested in this rule set:

- Block Applications in Request Cycle
- Block Applications in Response Cycle

Block Applications in Request Cycle

This nested rule set handles application filtering in the request cycle.

Nested library rule set – Block Applications in Request Cycle
Criteria – *Always*
Cycle – Requests (and IM)

The rule set contains the following rules:

Block instant messaging applications

Application.Name is in list Instant Messaging –> Block<Default>

The rule uses the *Application.Name* property to check whether the name of an application is contained in a specified list. If it is, it blocks a request for this application.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

Block web applications with high risk

Application.HighRisk equals true AND Application.Name is in list Web Browsing and Web Conferencing –> Block<Default>

The rule uses the *Application.HighRisk* property to check the reputation score of an application and the *Application.Name* property to check whether the name of this application is contained in a specified list. If the reputation score reaches or exceeds the high-risk level and the application name is also on the list, it blocks a request for this application.

The action settings specify a message to the requesting user.

Block Facebook chat

Application.ToString (Application .Name) equals "Facebook.Chat" –> Block<Default>

The rule uses the *Application.To String* property to check whether the name of an application is equal to a specified string. For this purpose, the name of the application is converted into a string. If the converted application name equals the specified string, a request for the application is blocked.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

Block Applications in Response Cycle

This nested rule set handles application filtering in the response cycle.

Nested library rule set – Block Applications in Response Cycle
Criteria – *Always*
Cycle – Responses

The rule set contains the following rule:

Applications to be looked for in response cycle

Application.Name is in listt of Applications to Search for in Response Cycle –> Block<Default>

The rule uses the *Application.Name* property to check whether the name of an application is contained in a specified list. If it is, it blocks a request for this application.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

Block web applications with high risk

Application.HighRisk equals true AND Application.Name is in list Web Browsing and Web Conferencing –> Block<Default>

The rule uses the *Application.HighRisk* property to check the reputation score of an application and the *Application.Name* property to check whether the name of this application is contained in a specified list. If the reputation score reaches or exceeds the high-risk level and the application name is also on the list, it blocks a request for this application.

The action settings specify a message to the requesting user.

Block Facebook chat

Application.ToString (Application .Name) equals "Facebook.Chat" –> Block<Default>

The rule uses the *Application.To String* property to check whether the name of an application is equal to a specified string. For this purpose, the name of the application is converted into a string. If the converted application name equals the specified string, a request for the application is blocked.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

Streaming media filtering

Streaming media filtering ensures that the users of your network cannot access streaming media if you do not want it. The filtering detects whether web objects are streaming media and blocks access accordingly.

The following elements are involved in this process:

- A filtering rule that controls the process
- A module that calculates the probability for web objects that they are streaming media

Streaming media filtering is usually applied in the response cycle of the filtering process to block streaming media sent by web servers in response to user requests.

Rule for streaming detection

To block web objects that are streaming media with a given probability you can set up a rule that uses the *StreamDetector.IsMediaStream* property. If the value of this property is true, access to a web object is blocked, as, for example, the following rule does it.

Name

Block access to streaming media

Criteria		Action
StreamDetector.IsMediaStream<Streaming Detection> equals true	–>	Block<Streaming Media Blocked>

The value of the *StreamDetector.IsMediaStream* property is provided by the Stream Detector module.

When this property is set to true, two additional properties are given related values. The value of the *StreamDetector.Probability* property is the percentage that was actually calculated for a web object, for example, 60 or 70.

The value of the *StreamDetector.MatchedRule* property is the name of the rule that matched.

You can use these additional properties in rules that record information in log file entries.

Streaming media filtering is not performed by default on an appliance. If you want to have it done, you need to create a rule like the one described above.

We recommend to use this rule not in a rule set of its own, but to insert it into another, suitable rule set, for example, in a media type filtering rule set.

Module for streaming detection

The probability that web objects are streaming media is calculated by the *Stream Detector* module (also known as filter or engine), which uses information about URL categories, content-type headers, source IP addresses, and other items for its calculation. The result of a probability calculation is a percentage.

The types of streaming media that can be detected in this way include the following:

- Flash-based video
- IC9 streams
- MS WMSP
- RealMedia
- MP3 streams

You can configure settings for this module and name them, for example, *Streaming Detection*. The settings include the minimum value for the probability that a web object is streaming media.

Configure streaming media filtering

You can configure streaming media filtering to adapt this process to the needs of your network.

Complete the following high-level steps.

Task

1. Create a streaming media filtering rule that blocks web objects if the probability that they are streaming media reaches or exceeds a configured level.
2. Insert this rule in a suitable rule set, for example, in a media type filtering rule set.

   You can modify the rule later on by increasing or reducing the probability level. This is done by configuring the settings of the Stream Detector module.
3. Save your changes.

Configure the streaming detection module

You can configure the module that calculates the probability for a given web object that it is streaming media.

Task

1. Select **Policy** | **Settings**.
2. Select **Stream Detector** and click **Add**.

   The **Add Settings** window opens.
3. In the **Name** input field, type a name for the settings.
4. [Optional] In the **Comment** input field, type a comment on the settings.
5. [Optional] Click the **Permissions** tab and configure who is allowed to access the settings.
6. Under **Streaming Detector**, configure settings for the module as needed.
7. Click **Save Changes**.

See also
Stream Detector settings on page 219

Stream Detector settings

The Stream Detector settings are used to configure the module that calculates the probability for web objects that they are streaming media.

Streaming Detector

Setting for the module that calculates streaming media probabilities

Table 10-12 Streaming Detector

Option	Definition
Minimal probability	Minimum value (in percent, specified by a number from 0 to 100) for the probability that a web object is streaming media

Global whitelisting

Global whitelisting ensures that all further filtering is skipped for the objects that are whitelisted, so access to them cannot be blocked.

The following elements are involved in this process:

- Filtering rules that control the process
- Whitelists that are used by rules to exempt particular web objects from further filtering

Filtering rules

The rules that control global whitelisting are usually contained in one rule set.

Whitelisting rules are placed and processed in this rule set. If any of them applies, the following rule sets are skipped and no further filtering is performed for the whitelisted objects.

You can review these rules, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for global whitelisting is included. Its name is *Global Whitelist*.

Whitelists

Whitelists are used by whitelisting rules to let particular web objects skip further filtering. There can be whitelists for URLs, media types, and other types of objects.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the whitelisting rules.

Configure global whitelisting

You can configure global whitelisting to adapt this process to the needs of your network.

Complete the following high-level steps.

Task

1. Review the rules in the rule set for global whitelisting.

   By default, this is the *Global Whitelisting* rule set.

2. Modify these rules as needed.

You can, for example, do the following:

- Enable or disable whitelisting rules
- Edit the lists used by the whitelisting rules

  A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

- Create whitelists of your own and let them be used by the whitelisting rules

3 Save your changes.

Global Whitelist rule set

The Global Whitelist rule set is the default rule set for global whitelisting.

Default rule set – Global Whitelist
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The rule set contains the following rules.

Client IP is in list Allowed Clients

Client.IP is in list Allowed Clients –> Stop Cycle

The rule uses the *Client.IP* property to check whether the IP address of a client that a request was sent from is on the specified whitelist.

If it is, the rule applies and stops the current processing cycle. The request is then forwarded to the appropriate web server.

URL.Host matches in list Global Whitelist

URL.Host matches in list Global Whitelist –> Stop Cycle

The rule uses the *URL.Host* property to check whether the host that a URL sent in a request provides access to is on the specified whitelist.

If it is, the rule applies and stops the current processing cycle. The request is then forwarded to the web server that is the requested host.

SSL scanning

SSL scanning ensures that SSL-secured web traffic can be processed and made available to other filtering functions.

The following elements are involved in the SSL scanning process:

- SSL scanning rules that control the process
- Whitelists and other lists that are used by the rules to exempt web objects from SSL scanning and to perform other functions within the process
- Modules that are called by the rules to perform certificate verification and other functions within the process

SSL scanning rules

The rules that control SSL scanning are usually contained in one rule set that has several nested rule sets. Each of the nested rule sets controls a particular function of the SSL scanning process:

- **Handle the CONNECT call** — There is a rule set with rules for handling the CONNECT call, which is sent at the beginning of SSL-secured communication under the HTTPS protocol.
- **Verify certificates** — There are rule sets for verifying certificates that are submitted by clients and servers in SSL-secured communication, for example, by verifying the common names in these certificates.

  This part of the process allows verification for both explicit proxy and transparent setups.
- **Enable content inspection** — Another rule set contains rules for enabling the inspection of content that is transferred in SSL-secured communication.

To find out whether an object is infected, the rule calls the Anti-Malware module, which scans the object and lets the rule know about the result.

Whitelisting rules can be placed and processed in this rule set before the blocking rule. If any of them applies, the blocking rule is skipped and the whitelisted objects are not scanned.

You can review the rules that are implemented on the appliance for SSL scanning, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for SSL scanning is included. Its name is *SSL Scanner*. However, the rule set is not enabled initially.

Whitelists and other lists for SSL scanning

Whitelists are used by the SSL scanning rules to let web objects skip parts of the process. For example, a certificate whitelist exempts certificates from undergoing verification.

Other lists used in SSL scanning contain the port numbers that are allowed in CONNECT calls if these are to be accepted or the servers that require a special kind of certificate verification because a particular method of exchanging keys cannot be applied on them.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the SSL scanning rules.

Modules for SSL scanning

The following modules (also know as *engines*) are called by the SSL scanning rules to perform different parts of the SSL scanning process:

- **SSL Scanner** — Handles certificate verification or the enabling of content inspection, depending on the settings it runs with.

  Accordingly, the module is called by the rules for certificate verification and content inspection with different settings.

- **Modules for setting the client context** — Handle the submitting of a certificate for the appliance to the clients that send requests to it in SSL-secured communication.

  When this certificate is submitted, the certificate authority (CA) that issued the certificate can be sent with it or not. Accordingly, there is a module for submitting a certificate *with* and another module for submitting a certificate *without* its certificate authority.

  The SSL Scanner rule set of the default system, uses the method of submitting a certificate with its certificate authority.

  A default certificate authority is available for use after the initial setup. However, we recommend that you provide a certificate authority of your own for further use.

- **Certificate Chain** — Handles the building of a certificate chain

  When building the chain, the module uses a list of certificate authorities for the certificates that are included in the chain. You can add certificate authorities to existing lists and also add new lists.

Configure SSL scanning

You can configure SSL scanning to adapt this process to the needs of your network.

Complete the following high-level steps.

Task

1. Enable the rule set for SSL scanning and review the rules in this rule set.

   By default, this is the *SSL Scanner* rule set.

2. Modify these rules as needed.

   You can, for example, do the following:

   - Replace the default root certificate authority (CA) for signing certificates that the appliance sends to its clients by a certifcate of your own.

     This can be a certificate authority that you create yourself on the user interface or one that you import from your file system.

   - Enable or disable whitelisting rules, for example:
     - The default rule for skipping certificate verification when a certificate that was submitted by a client is on a whitelist
     - The default for skipping content inspection when the host of a requested URL is on a whitelist
   - Edit the lists used by the whitelisting rules

     A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

   - Create whitelists of your own and let them be used by the whitelisting rules

- Modify the settings of the modules involved in SSL scanning.
    - SSL Scanner module
    - SSL Client Context module
    - Certificate Chain module

3 Save your changes.

Configure the modules for SSL scanning

You can configure the modules for SSL scanning to modify the way SSL-secured web traffic is processed.

The following modules are involved in SSL scanning and can be configured:

- SSL Scanner module
- SSL Client Context module
- Certificate Chain module

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, find the rule set for SSL scanning.

By default, this is the *SSL Scanner* rule set.

3 Expand the rule set and select the nested rule set that contains the rule with the settings for the module you want to configure.

For example, to configure the SSL Scanner module, expand the nested *Handle CONNECT Call* rule set. It contains by default the rule *Enable certificate verification* with the *Default certificate verification* settings for the SSL Scanner module.

The rules of the nested rule set appear on the settings pane.

4 Make sure **Show details** is selected.

5 Find the rule with the settings for the module you want to configure.

This could be, for example, the *Enable certificate verification* rule that was mentioned above.

6 Within the rule, click a settings name.

For example, in the rule event of *Enable certificate verification*, click *Default certificate verification*.

The **Edit Settings** window opens. It provides the settings for a module, for example, the SSL Scanner module.

7 Configure these settings as needed.

8 Click **OK** to close the window.

9 Click **Save Changes**.

See also

SSL Scanner settings on page 228
SSL Client Context settings on page 229
Certificate Chain settings on page 229

Replace the default root certificate authority

You can replace the default root certificate authority that is provided after the nitial setup for signing the certificates that the appliance sends to its clients by a certificate authority of your own.

You can create a new root certificate authority on the user interface or import one from your file system.

Tasks

- *Create a root certificate authority* on page 224
  You can create a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.
- *Import a root certificate authority* on page 224
  You can import a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.

Create a root certificate authority

You can create a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.

Task

1. Select **Policy** | **Settings**.
2. On the **Engines** branch of the settings tree, go to **SSL Client Context with CA** and select the settings you want to use the new certificate authority for.
3. Click **Generate New**.

   The **Generate New Certificate Authority** window opens.
4. In the **Organization** and **Locality** fields, type suitable information for your own certificate authority.
5. [Optional] In the **Organizational unit** and **State** fields, type suitable information. From the **Country** list, select a country.
6. In the **Common name** field, type a common name for your own certificate authority.
7. [Optional] In the **Email address** field, type an email address of your organization.
8. From the **Valid for** list, select the time that your certificate authority should be valid.
9. [Optional] In the **Comment** field, type a plain-text comment on the certificate authority.
10. Click **OK**.

    The new certificate authority is generated.
11. Click **Save Changes**.

Import a root certificate authority

You can import a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.

Task

1. Select **Policy** | **Settings**.
2. On the settings tree, select **SSL Client Context with CA** and click the settings you want to use the imported certificate authority for.

3 Click **Import**.

The **Import Certificate Authority** window opens.

4 Enter the name of the certificate authority file in the **Certificate** field by clicking **Browse** and browsing to a suitable file.

The file must be encoded in PEM (Privacy-enhanced mail) format.

5 Enter the name of the certificate key file in the **Private key** key field by clicking **Browse** and browsing to a suitable file.

The file must be encoded in PEM format. The key must have a length of at least 2048 bit.

6 [Conditional] If the private key is protected by a password, type it in the **Password** field.

Only unencrypted keys and key that are AES-128-bit encrypted can be used here.

7 [Conditional] If the certificate authority is part of a certificate chain and you want to provide information on this chain with the certificate, enter the name of the file containing the information in the **Certificate chain** field by clicking **Browse** and browsing to a suitable file.

The file must be encoded in PEM format.

8 Click **OK**.

The certificate authority is imported.

9 Click **Save Changes**.

Client certificate list

The client certificate list is a list of certificates that can be sent to a web server when a client request is received on an appliance in SSL-secured communication and passed on to the appropriate web server.

The certificate is sent when the web server asks for it at the initial and subsequent handshakes, as SSL renegotiation is performed.

A rule event tells the appliance to use a client certificate for communication with the web server. The certificate can then be selected from the client certificate list.

In this case, the private key for the certificate must be provided by the client that sent the request.

Alternatively, a preconfigured certificate can be used that is always sent to the web server.

The rule event that triggers the use of a certificate from the client certificate list can belong to rules that apply to CONNECT requests (even in transparent setups) or to rules in rule sets for certificate verification that have CERTVERIFY as value for the *Command.Name* property in their criteria.

You can configure settings for the rule event that include a client certificate list and the instruction to use it. The settings can also specify that the private key for the certificates that the clients of the appliance provide is stored unencrypted.

Create a client certificate list

You can create a list of client certificates that can be sent to web servers in SSL-secured communication.

Task

1 Select **Policy** | **Settings**.

2 On the settings tree, select **SSL Client Certificate Handling** and click **Add**.

The **Add Settings** window opens with the **Add Settings** tab selected.

3 Configure general settings parameters.

  a In the **Name** field, type a name for the settings.

  b [Optional] In the **Comments** field, type a plain-text comment on the settings.

  c [Optional] Click the **Permissions** tab and configure who is allowed to access the settings.

4 Under **Client Certificate Handling**, make sure the option **Use client certificate from Known client certificates list if client has proven ownership** is selected.

5 On the toolbar of the **Known client certificates** list, click **Add**.

The **Add Client Certificate** window opens.

6 Click **Import** to import a client certificate.

The **Import Client Certificate** window opens.

7 Import a client certificate.

  a Next to the **Certificate** field, click **Browse**, and within the local file manager that opens, browse to a suitable certificate file and select it.

  The file manager closes and the certificate file name appears in the field.

  b Next to the **Private key** field, click **Browse**, and within the local file manager that opens, browse to a suitable key file and select it.

  The file manager closes and the key file name and password appear in the **Private key** and **Password** fields.

  c Click **OK**.

  The window closes and the certificate file information appears in the **Import Client Certificate** window.

  d [Optional] In the **Comments** field, type a plain-text comment on the certificate.

8 Click **OK**.

The **Add Client Certificate** window closes and the certificate file name and comment (if provided) appear in the **Known client certificates** list.

Repeat Steps 5 to 8 for any other certificate you want to add to the list.

9 Click **OK** to close the **Add Settings** window.

10 Click **Save Changes**.

SSL Client Certificate Handling settings

The SSL Client Certificate Handling settings are used for configuring client certificates that are sent to web servers in SSL-secured communication.

SSL Client Certificate Handling

Settings for configuring SSL client certificates

Table 10-13 SSL Client Certificate Handling

Option	Definition
Use client certificate from Known client certificates list if client has proven ownership	When selected, the client certificate that is sent to a web server in SSL-secured communication is taken from the list of known client certificates. However, the certificate is only taken from this list if it is proven that the client whose request the appliance forwards to a server is the owner of this certificate. After selecting this radio button, the **Known Client Certificates** section appears, which provides settings for configuring a list of certificates.
Always use predefined client certificate	When selected, the same client certificate is always sent to a web server in SSL-secured communication. After selecting this radio button, the **Predefined Client Certificate** section appears, which provides settings for configuring a single certificate

Known client certificates

Settings for configuring a list of known client certificates that can be sent to a web server

Table 10-14 Known client certificates

Option	Definition
List of known client certificates	List of client certificates that can be sent to a web server in SSL-secured communication

The following table describes the elements of an entry in the list of known client certificates.

Table 10-15 Known client certificates – List entry

Option	Definition
Certificate	Name of a client certificate
Comment	Plain-text comment on a certificate

Predefined client certificate

Settings for configuring a client certificate that is always sent to a web server

Table 10-16 Predefined client certificate

Option	Definition
Subject, **Issuer**, **Validity**, **Extensions**	Information on the client certificate that is currently used for sending to a web server
Import	Opens the **Import Client Certificate** window for importing a client certificate. After the import, information on the client certificate appears under **Subject**, **Issuer**, and in the other information fields.
Export	Opens your local file manager to let you store a client certificate in a suitable location.
Export Key	Opens your local file manager to let you store the private key for a client certificate in a suitable location.
Certificate Chain	Displays a certificate chain if one has been imported with a client certificate.

SSL Scanner settings

The SSL Scanner settings are used for configuring the way certificates are verified and content inspection is enabled for SSL-secured web traffic.

Enable SSL Scanner

Settings for configuring certificate verification or the enabling of content inspection

Table 10-17 Enable SSL Scanner

Option	Definition
SSL scanner function	Function performed by the SSL Scanner module • **Certificate verification** — When selected, the module verifies certificates submitted in SSL-secured communication. For the Default Certificate Verification and Certificate Verification Without EDH settings, this option is enabled by default. • **SSL inspection** — When selected, the module inspects the content of web objects transmitted in SSL-secured communication.
SSL protocol version	When selected, the module inspects the content of web objects transmitted in SSL-secured communication. • **TLS 1.0** — When selected, TLS (Transport Layer Security) version 1.0 is used. • **SSL 3.0** — When selected, SSL version 3.0 is used .
Server cipher list	String of Open SSL symbols used for decrypting server data The SSL Scanner module uses different strings for default certificate verification and for verifying certificates from servers that do not support the EDH (Ephemeral Diffie-Hellman) method.
SSL session cache TTL	Time (in seconds) for keeping the parameter values of a session in SSL-secured communication stored in the cache
Allow handshake and renegotiation with servers that do not implement RFC 5746	When selected, the SSL Scanner module performs these activities also in communication with web servers that fail to comply with the specified standard.

Allow Alternative Handshakes

Settings for handshakes in SSL-secured communication that use alternative parameter values

Table 10-18 Allow Alternative Handshakes

Option	Definition
Use alternative handshake settings after handshake failure	When selected, the SSL Scanner module uses alternative parameter values after the first attempt to perform a handshake in SSL-secured communication has failed.
SSL protocol version	Version of the protocol the SSL Scanner module follows when it performs an alternative handshake • **TLS 1.0** — When selected, TLS (Transport Layer Security) version 1.0 is used • **SSL 3.0** — When selected, SSL version 3.0 is used
Server cipher list	String of Open SSL symbols used for decrypting server data The SSL Scanner module uses different strings for default certificate verification and for verifying certificates from servers that do not support the EDH (Ephemeral Diffie-Hellman) method.

SSL Client Context settings

The SSL Client Context settings are used for the module that handles the certificates the appliance sends to its clients.

Define SSL Client Context

Settings for the certificate the appliances sends to its clients

Table 10-19 Enable SSL Scanner

Option	Definition
(Current root certificate authority)	Parameters and values of the root certificate authority (root CA) that is currently in use on the appliance After the initial setup, a default root CA is implemented on the appliance. For further administration, we recommend that you create your own root CA. Use the Generate New button to create this certificate authority.
Send certificate chain	When selected, the appliance sends information on the chain of certificates that are involved in the process of validating the certificate the appliance sends to its clients. The certificate the appliance sends as a server to its clients is considered to exist on level 0. When a certificate authority (CA) signs this server certificate to validate it, it is done on level 1. When an additional certificate authority validates the first certificate authority, it is done on level 2. With each additional certificate authority that is involved, the level increases by one.
Certificate chain	Input field for entering information on a certificate chain After importing an existing certificate authority (CA) that is involved in a certificate chain, the information on this certificate chain appears in the field.
Perform insecure renegotations	When selected, the module renegotiates the parameters for the SSL-secured communication even if this is insecure to do.
Client cipher list	String of Open SSL symbols used for decrypting client data
SSL session cache TTL	Time (in seconds) for keeping the parameter values of a session in SSL-secured communication stored in the cache
SSL protocol version	Version of the protocol the SSL Scanner module follows when it performs a handshake • **TLS 1.0** — When selected, TLS (Transport Layer Security) version 1.0 is used • **SSL 3.0** — When selected, SSL version 3.0 is used

Certificate Chain settings

The Certificate Chain settings are used for configuring the module that handles the building of certificate chains.

Certificate Verification

Settings for building a chain of certificates

Table 10-20 Certificate Verification

Option	Definition
List of certificate authorities	List for selecting a list of certificate authorities (CAs) that sign the certificates in a certificate chain

The following table describes the elements of a list entry

Table 10-21 List of certificate authorities

Option	Definition
Certificate authority	Name of a certificate authority
Certificate revocation list	List with information on when a certificate signed by this certificate authority becomes invalid and the URI used to access the list
Trusted	Information on whether a certificate authority is trusted on the appliance
Comment	Plain-text comment on a certificate authority

SSL Scanner rule set

The *SSL Scanner* rule set is the default rule set for SSL scanning.

Default rule set – SSL Scanner
Criteria – *Always*
Cycles – Requests (and IM)

The following rule sets are nested in this rule set:

- Handle CONNECT Call
- Certificate Verification
  - Verify Common Name (proxy setup)
- Content Inspection
- Verify Common Name (transparent setup)

Handle CONNECT Call

This nested rule set handles the CONNECT call in SSL-secured communication and enables certificate verification.

Nested library rule set – Handle CONNECT Call
Criteria – *Command.Name equals "CONNECT"*
Cycles – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is received on the appliance that contains the CONNECT command, which is sent in the opening phase of SSL-secured communication.

The rule set contains the following rules:

Set client context

Always –> Continue – Enable SSL Client Context with CA <Default CA>

The rule enables the use of a server certificate that is sent to a client.

The event settings specify the McAfee Web Gateway root certificate authority (CA), which is implemented on the appliance after the initial setup, as the default issuer of this certificate.

The Continue action lets processing continue with the next rule.

Tunneled hosts

URL.Host is in list SSL Host Tunnel List –> Stop Cycle

The rule lets requests for access to hosts with a URL that is on the specified whitelist skip SSL scanning.

Restrict destination ports to Allowed CONNECT Ports

URL.Port is not in list Allowed Connect Ports –> Block<Connect not allowed>

The rule blocks requests with destination ports that are not on the list of allowed CONNECT ports.

The action settings specify a message to the requesting user.

Enable certificate verification without EDH for hosts in no-EDH server list

URL.Host is in list No-EDH server –> Block<Connect not allowed> Stop Rule Set – Enable SSL Scanner<Certificate Verification without edh>

The rule enables the certificate verification for requests sent from a host on the no-EDH (Ephemeral Diffie-Hellman) server list.

The action settings specify a message to the requesting user.

The event settings specify running in verification mode for the SSL Scanner module and a special cipher string for data encryption on non-EDH hosts.

Enable certificate verification

Always –> Stop Rule Set – Enable SSL Scanner<Default certificate verification>

The rule enables certificate verification.

The event settings specify that the SSL Scanner module runs in verification mode.

Certificate Verification

This nested rule set handles the CERTVERIFY call in SSL-secured communication. It lets whitelisted certificates skip verification and blocks others according to particular criteria.

Nested library rule set – Certificate Verification
Criteria – *Command.Name equals "CERTVERIFY**
Cycles – Requests (and IM)

The rule criteria specifies that the rule set applies if a request is received on the appliance that contains the CERTVERIFY command, which is sent to request the verification of a certificate.

The following rule set is nested in this rule set:

- Verify Common Name (proxy setup)

The rule set contains the following rules:

Skip verification for certificates found in Certificate Whitelist

SSL.Server.Certificate.HostAndCertificate is in list Certificate Whitelist –> Stop Rule Set

cThe rule lets whitelisted certificates skip verification.

Block self-signed certificates

SSL.Server.Certificate.SelfSigned equals true –> Block <Certificate incident>

The rule blocks requests with self-signed certificates.

The action settings specify a message to the requesting user.

Block expired server (7 day tolerance) and expired CA certificates

SSL.Server.Certificate.DaysExpired greater than 7 OR SSL.Server.CertificateChain.ContainsExpiredCA<Default> equals true –> Block <Certificate incident>

The rule blocks requests with expired server and CA certificates.

The action settings specify a message to the requesting user.

Block too long certificate chains

SSL.Server.CertificateChain.PathLengthExceeded<Default> equals true –> Block <Certificate incident>

The rule blocks a certificate chain if it exceeds the path length.

The settings in the property specify a list for the module that checks the certificate authorities.

The action settings specify a message to the requesting user.

Block revoked certificates

SSL.Server.CertificateChain.ContainsRevoked<Default> equals true –> Block <Certificate incident>

The rule blocks a certificate chain if one of the included certificates has been revoked.

The settings in the property specify a list for the module that checks the certificate authorities.

The action settings specify a message to the requesting user.

Block unknown certificate authorities

SSL.Server.CertificateChain.FoundKnownCA<Default> equals false –> Block <Certificate incident>

The rule blocks a certificate chain if none of the certificate authorities (CAs) issuing the included certificates is a known CA .

The settings in the property specify a list for the module that checks the certificate authorities.

The action settings specify a message to the requesting user.

Block untrusted certificate authorities

SSL.Server.FirstKnownCAIsTrusted<Default> equals false –> Block <Certificate incident>

The rule blocks a certificate chain if the first known CA that was found is not trusted.

The settings in the property specify a list for the module that checks the certificate authorities.

The action settings specify a message to the requesting user.

Verify Common Name (proxy setup)

This nested rule set verifies the common name in a certificate. It applies to requests sent in explicit proxy mode.

Nested library rule set – Verify Common Name (proxy setup)
Criteria – *Connection.SSL.TransparentCNHandling equals false*
Cycles – Requests (and IM)

The rule criteria specifies that the rule set applies if a request is received on a connection used in SSL-secured communication and verification of the common name is not performed in transparent mode.

The rule set contains the following rules:

Allow matching hostname

URL.Host equals Certificate.SSL.CN –> Stop Rule Set

The rule allows a request if the URL of the requested host is the same as the common name in the certificate.

Allow wildcard certificates

Certificate.SSL.CN.HasWildcards equals true AND URL.Host matches.Certificate.SSL.CN.ToRegex(Certificate.SSL.CN) –> Stop Rule Set

The rule allows requests to hosts sending certificates that have wildcards in their common names matching the URLs of the hosts.

To verify that a common name containing wildcards matches a host, this name is converted into a regular expression.

Allow alternative common names

URL.Host is in list Certificate.SSL.AlternativeCNs –> Stop Rule Set

The rule allows requests to hosts with alternative common names in their certificates and the host matches at least one of them.

Block incident

Always –> Block <Common name mismatch>

If any of the rules for allowing matching common names applies, processing of the rule set stops and this rule is not processed. Otherwise, requests are blocked by this rule because it is then a common name mismatch.

The action settings specify a message to the requesting user.

Content Inspection

This nested rule set completes the handling of a CERTVERIFY call. It lets some requests skip content inspection according to particular criteria and enables inspection for all others.

Nested library rule set – Content Inspection
Criteria – *Command.Name equals "CERTVERIFY**
Cycles – Requests (and IM)

The rule criteria specifies that the rule set applies if a request is received on the appliance that contains the CERTVERIFY command, which is sent to request the verification of a certificate.

The rule set contains the following rules:

Skip content inspection for hosts found in SSL Inspection Whitelist

Connection.SSL.Transparent equals false AND URL.Host matches in list SSL Inspection Whitelist –> Stop Rule Set

The rule lets requests sent to whitelisted hosts skip content inspection. It applies only in non-transparent mode.

Skip content inspection for CN found in SSL Inspection Whitelist

Connection.SSL.Transparent equals true AND Certificate.SSL.CN matches in list SSL Inspection Whitelist –> Stop Rule Set

The rule lets requests with whitelisted common names in their certificates skip content inspection. It applies only in transparent mode.

The rule is not enabled initially.

Do not inspect connections with client certificates

Connection.Client.CertificateIsRequested equals true –> Stop Rule Set

The rule lets requests skip inspection if they require the use of client certificates.

The rule is not enabled initially.

Enable content inspection

Always –> Continue – Enable SSL Scanner<Enable content inspection>

The rule enables content inspection.

The event settings specify that the SSL Scanner module runs in inspection mode.

If any of the rules for skipping content inspection applies, processing of the rule set stops and this last rule, which enables the inspection, is not processed. Otherwise, content inspection is enabled by this rule.

Verify Common Name (transparent setup)

This nested rule set verifies the common name in a certificate. It applies to requests sent in explicit proxy mode. It applies only to requests sent in transparent mode.

With requests sent in explicit proxy mode, the host name that is compared to the common name is taken from the CONNECT request that a client sends.

As in transparent mode no CONNECT request is sent, the host name is taken from the request for web access that a client sends.

Nested library rule set – Verify Common Name (transparent setup)
Criteria – *Connection.SSL.TransparentCNHandling equals true AND Command.Name does not equal "CONNECT" AND Command.Name does not equal "CERTVERIFY"*
Cycles – Requests (and IM)

The rule criteria specifies that the rule set applies if a request is received on a connection used in SSL-secured communication and verification of the common name is performed in transparent mode.

The rule set contains the following rules:

Allow matching hostname

URL.Host equals Certificate.SSL.CN –> Stop Rule Set

The rule allows a request if the URL of the requested host is the same as the common name in the certificate.

Allow wildcard certificates

Certificate.SSL.CN.HasWildcards equals true AND URL.Host matches.Certificate.SSL.CN.ToRegex(Certificate.SSL.CN) –> Stop Rule Set

The rule allows requests to hosts sending certificates that have wildcards in their common names matching the URLs of the hosts.

To verify that a common name containing wildcards matches a host, this name is converted into a regular expression.

Allow alternative common names

URL.Host is in list Certificate.SSL.AlternativeCNs –> Stop Rule Set

The rule allows requests to hosts with alternative common names in their certificates and the host matches at least one of them.

Block incident

Always –> Block <Common name mismatch>

If any of the rules for allowing matching common names applies, processing of the rule set stops and this rule is not processed. Otherwise, requests are blocked by this rule because it is then a common name mismatch.

The action settings specify a message to the requesting user.

Data loss prevention

Data loss prevention (DLP) ensures that sensitive content is not allowed to leave your network. The prevention process detects this content and blocks traffic going out to the web accordingly.

The following elements are involved in this process:

- Data loss prevention rules that control the process
- Default classifications and a dictionary that you fill with entries for data loss prevention
- Data loss prevention modules, which are called by the rules that are processed to find out about sensitive content

You can also use data loss prevention rules to keep inappropriate content from entering your network. However, this can have an impact on performance.

The data loss prevention process can be applied to text contained in the body that is sent with a request or response or to any other text that is contained in requests or responses, for example, URL parameters or headers.

When you are running the appliance together with a DLP solution that uses an ICAP server for the filtering process, you can implement a rule set to ensure the smooth flow of data between the appliance and the ICAP server.

Data loss prevention rules

Data loss prevention is not implemented by default on the appliance, but you can import the *Data Loss Prevention* rule set from the library.

You can then review the rules of this rule set, modify or delete them, and also create your own rules.

A data loss prevention rule blocks, for example, a request if the text that is sent as its body includes sensitive content. To find out whether this is true for a given request body, the rule calls a module that inspects the body. To know what is considered sensitive, the module refers to the default classifications on the system lists or to dictionary entries, according to what is configured.

When a request or response is processed, its body text is stored as the value of the *Body.Text* property. Before body text can be stored and inspected, it must be extracted. The Composite Opener module performs the opening jobs. A rule in a rule set of the *Common Rules* rule set enables the opener by default.

A request body could, for example, be a text file that uploading to the web is requested for. The value of a suitable body-related property in the rule criteria would then have to be true for the rule to apply and execute the blocking.

The following rule uses the *DLP.Classification.BodyText.Matched* property in this way. If a request includes sensitive content in its body, this is detected by the data loss prevention module. The value of the property is set to *true*, and the request is blocked.

Name

Block files with SOX information

Criteria		Action
DLP.Classification.BodyText.Matched<SOX> equals true	–>	Block<DLP.Classification.Block>

When this rule is processed, the data loss protection module knows, due to its settings, that it has to look for content that is sensitive with regard to the SOX (Sarbanes-Oxley) regulations, which deal with responsibilities of public companies.

Events can be added to the rule to log information on data loss prevention or to increment a counter that counts how often it has occurred that a request is blocked due to this rule.

Default classifications and dictionary entries

Default classifications and dictionary entries are used in data loss prevention to specify sensitive content that should be prevented from leaving your network.

However, you can also system lists and dictionary entries to specify inappropriate content, such as discriminatory or offensive language, that should not be allowed to enter your network. Inappropriate content could, for example, be specified this way to let a rule block content sent from web servers in response to requests.

The library rule set for data loss prevention contains a nested rule set for processing body text in the response cycle.

Default classifications and dictionary entries differ in the following ways:

- **Default classifications** — Provide information for detecting different kinds of sensitive or inappropriate content, for example, credit card numbers, social security numbers, or medical diagnosis data.

  Default classifications are contained in folders and subfolders on system lists and updated by the appliance system. You can view the system lists under **DLP Classification** in the **System Lists** branch of the lists tree, but you cannot edit or delete them.

  When you edit the settings of the module that handles classifications, you can select suitable subfolders from the folders on these lists and create a list with classifications for data loss prevention in your network.

- **Dictionary entries** — Specify sensitive or inappropriate content, for example, names of persons or keywords indicating content that should not leave your network

  The dictionary is created as part of the settings for the module that handles this list.

  Creating a dictionary and filling it with entries for sensitive or inappropriate content is a means to configure the data loss prevention process beyond what is possible by using the default classifications on the system lists. This way you can adapt the process to the requirements of your network.

Data loss prevention modules

The job of the data loss prevention modules (also known as *engines*) is to detect sensitive or inappropriate content in the body text of requests and responses and also in any other text that is sent with requests and responses.

When composite objects, such as archive documents, bodies of POST requests, and others, are sent with requests or responses, they are also included in the data loss prevention process. To account for such objects, the data loss prevention rules are also processed in the embedded objects cycle.

Depending on what the data loss prevention modules find out, body-related properties in rule criteria are set to *true* or *false*, so web traffic is eventually blocked or allowed.

There are two modules that differ in their use of lists for detecting relevant content:

- **Data Loss Prevention (Classifications)** — Uses default classifications on system lists for data loss prevention
- **Data Loss Prevention (Dictionaries)** — Uses dictionaries with entries for sensitive and inappropriate content that you provide yourself for data loss prevention

When configuring settings for the modules, you let them know which content to look for. The default classifications and dictionary entries that specify the content are among the settings parameters.

Search methods for data loss prevention

There are different methods of searching content that should be prevented from leaving or entering your network.

- A search can aim at finding out whether a given request or response body includes portions of content that are specified as sensitive or inappropriate.
- A search can begin with a portion of content, for example, an URL parameter or header, and find out whether it is sensitive or inappropriate according to what you have configured.

For the first method, you can use the *DLP.Classification.BodyText.Matched* property that was already shown in a sample rule.

For the second, you can use the *DLP.Classification.AnyText.Matched* property. This property takes a string parameter for the content portion that is checked for being on a system list or in a dictionary.

Depending on what you are working with, you would use the two already mentioned parameters with system lists and *DLP.Dictionaries.BodyText.Matched* and, *DLP.Dictionaries.AnyText.Matched* with the dictionary.

Logging data loss prevention

Additional properties are provided for logging the results of the data loss prevention process. They allow you to log this data, for example, using an event in a rule.

When the value of *DLP.Classification.BodyText.Matched* is *true* for the body text of a request or response that was processed, the following applies for the relevant logging properties:

- *DLP.Classification.BodyText.MatchedTerms* contains a list of the matching terms from the body text
- *DLP.Classification.BodyText.MatchedClassifications* contains a list of the matching classifications

When the value of *DLP.Dictionary.BodyText.Matched* is *true*, *DLP.Dictionary.BodyText.MatchedTerms* contains a list of all matching terms.

Similarly, matching terms and classifications can be logged for the search method that looks for matches of a given text string.

When the value of *DLP.Classification.AnyText.Matched* is *true*:

- *DLP.Classification.AnyText.MatchedTerms* contains a list of matching terms found in text other than body text.
- *DLP.Classification.AnyText.MatchedClassifications* contains a list of matching classifications found in text other than body text.

When the match is in a dictionary, *DLP.Dictionary.AnyText.Matched* is *true* and *DLP.Dictionary.AnyText.MatchedTerms* contains a list of matching terms.

Information on data loss prevention results is also shown on the dashboard.

Preventing loss of medical data

The following is an example of data loss prevention that assumes medical data must be prevented from leaving the network of an American hospital.

Default classifications for preventing the loss of medical data are contained in the HIPAA (Health Insurance Portability and Accountability Act) folder. In addition to this default information, the names of the doctors who are working in the hospital are entered in a dictionary to ensure they also do not leave the network.

The following activities need to be completed for configuring data loss prevention in this example:

- Configure settings for the Data Loss Prevention (Classifications) module that include the default HIPAA classifications
- Configure settings for the Data Loss Prevention (Dictionaries) module that include the doctors' names as dictionary entries
- Make sure the rule that activates the Composite Opener is enabled

  In the default rule set system, this rule is contained in the Enable Opener rule set, which is nested in the Common Rules rule set.
- Create a rule that checks content according to the configured settings

  The rule must be included in a rule set that applies in the request cycle for request to upload data from the hospital network to the web.

  This rule set can be a nested rule set of the default rule set for data loss prevention or a rule set that you create yourself.

  In this example, the rule checks only text contained in the body of a request. It could look as follows:

Name		
Prevent loss of HIPAA data and doctors' names		
Criteria		Action
DLP.Classification.BodyText.Matched<HIPAA> equals true AND *DLP.Dictionary.BodyText.Matched<Doctors'Names> equals true*	–>	Block<DLP.Classification.Block>

See also
List of properties on page 390

Configure data loss prevention

You can configure data loss prevention to keep sensitive content from leaving your network. You can also use it to keep inappropriate content from entering.

Complete the following high-level steps.

Task

1. Import the Data Loss Prevention rule set from the library.
2. Review its rules and modify them as needed.

   You can, for example:

   - Configure settings for data loss prevention using default classifications.
   - Configure settings for data loss prevention using dictionary entries.
   - Modify other settings parameters.
   - Create rules of your own.

   You can also create your own rule set for data loss prevention instead of using the library rule set.

3 Make sure the Composite Opener is enabled, so the body text sent with requests and responses can be inspected.

In the default rule set system, this rule is contained in the Enable Opener rule set, which is nested in the Common Rules rule set.

4 If you want to run data loss prevention with ICAP, you can import another rule set from the library and modify its rules as needed.

5 Save your changes.

Configure data loss prevention using default classifications

You can configure data loss prevention by selecting default classifications from system lists and entering them in a list that is included in the settings of the data loss prevention module for processing classifications.

Task

1 Select **Policy | Settings**.

2 On the settings tree, select **Data Loss Prevention (Classifications)** and click **Add.**

The **Add Settings** window opens.

3 Configure general settings parameters:

a In the **Name** field, type a name for the settings.

b [Optional] In the **Comment** field, type a plain-text comment on the settings.

c [Optional] Click the **Permissions** tab and configure who is allowed to access the settings.

4 On the toolbar of the **DLP Classifications** inline list, click the **Edit** icon.

An **Edit** window opens with a tree structure of folders containing subfolders with default classifications.

5 Expand a folder, for example, **SOX Compliance**, and select a subfolder, for example, **Compliance Reports**. Then click **OK**.

You can also select several subfolders of a folder at once, select folders from different subfolders, or select complete folders with all their respective subfolders.

The **Edit** window closes and the subfolder or subfolders appear in the **DLP Classifications** inline list.

6 Click **Save Changes**.

Configure data loss prevention using dictionary entries

You can enter text and wildcard expressions that specify sensitive or inappropriate content into as entries in a dictionary for data loss prevention.

After importing the library Data Loss Prevention rule set, use of a dictionary with entries specifying sensitive or inappropriate content is not yet implemented. You need to create appropriate settings to implement it and fill the dictionary with entries.

Tasks

- *Create settings with a dictionary* on page 240
  For data loss prevention that uses dictionary entries, you must create settings that include a dictionary.
- *Fill the dictionary with entries* on page 240
  After creating settings with a dictionary, you can fill the dictionary with entries.

Create settings with a dictionary

For data loss prevention that uses dictionary entries, you must create settings that include a dictionary.

Task

1. Select **Policy** | **Settings**.
2. On the settings tree, select **Data Loss Prevention (Dictionaries)** and click **Add**.

   The **Add Settings** window opens.
3. Configure general settings parameters:
   a. In the **Name** field, type a name for the settings.
   b. [Optional] In the **Comment** field, type a plain-text comment on the settings.
   c. [Optional] Click the **Permissions** tab and configure who is allowed to access the settings.

You can now fill the dictionary with entries.

Fill the dictionary with entries

After creating settings with a dictionary, you can fill the dictionary with entries.

Task

1. Within the settings you have created for data loss prevention using dictionary entries, click the **Add** icon on the toolbar of the **Dictionary** inline list.

   The **Add DLP Dictionary Entry** window opens.
2. Under **Type of data to search**, select **Text** or **Wildcard expression**.
3. In the **Text or wildcard expression** field, enter a text string or a wildcard expression.
4. [Optional] Specify additional information for an entry:
   - If you have entered a text string, select one of the following options or any combination of them:
     - **Case-sensitive**
     - **At start of word**
     - **At end of word**
   - If you have entered a wildcard expression, select **Case-sensitive** or leave it deselected as needed.
5. [Optional] In the **Comment** field, type a plain-text comment on an entry.
6. Click **OK**.

   The **Add DLP Dictionary Entry** window closes and the new entry appears in the dictionary.

   Repeat Steps 1 to 6 to add more entries.
7. Click **OK** in the **Add Settings** window.

   The window closes and the new settings appear on the settings tree under **Data Loss Prevention (Dictionaries)**.

Data Loss Prevention (Classifications) settings

The Data Loss Prevention (Classifications) settings are used for configuring entries in classification lists that specify sensitive or inappropriate content.

DLP Classifications Parameters

Settings for configuring the use of classification lists when searching for sensitive or inappropriate content

Table 10-22 DLP Classifications Parameters

Option	Definition
Tracking policy	Extent of the search for sensitive or inappropriate content in the body text of requests and responses • Minimum — The search stops after the first instance of sensitive or inappropriate content has been found. • Maximum — The search is continued until the last instance of sensitive or inappropriate content has been found.
DLP Classifications	List of entries in classification lists that you select from the system lists provided under **DLP Classification** on the lists tree

The following table describes an entry in the DLP Classifications list

Table 10-23 DLP Classifications Parameters – List entry

Option	Definition
DLP Classification	Entry providing information about detecting sensitive or inappropriate content
Comment	Plain-text comment on an entry

Advanced Parameters

Settings for configuring advanced functions for data loss prevention

Table 10-24 Advanced Parameters

Option	Definition
Reported context width	Maximum number of characters shown around a matching term in a list that is the value of the *DLP.Classification.Matched.Terms* property
Context list size	Maximum number of matching terms shown in a list that is the value of the *DLP.Classification.Matched.Terms* property

Data Loss Prevention (Dictionaries) settings

The Data Loss Prevention (Dictionaries) settings are used for configuring text and wildcard expressions that specify sensitive or inappropriate content.

DLP Dictionary Parameters

Settings for configuring text and wildcard expressions specifying sensitive or inappropriate content

Table 10-25 DLP Dictionaries Parameters

Option	Definition
Tracking policy	Extent of the search for sensitive or inappropriate content in the body text of requests and responses • **Minimum** — The search stops after the first instance of sensitive or inappropriate content has been found. • **Maximum** — The search is continued until the last instance of sensitive or inappropriate content has been found.
Dictionary	List of text strings and wildcard expressions specifying sensitive or inappropriate content

The following table describes an entry in the **Dictionary** list.

Table 10-26 Dictionary – List entry

Option	Definition
Text or wildcard expression	Text string or wildcard expression specifying sensitive or inappropriate content
Comment	Plain-text comment on a text string or wildcard expression

Advanced Parameters

Settings for configuring advanced functions for data loss prevention

Table 10-27 Advanced Parameters

Option	Definition
Reported context width	Maximum number of characters shown around a matching term in a list that is the value of the *DLP.Dictionary.Matched.Terms* property
Context list size	Maximum number of matching terms shown in a list that is the value of the *DLP.Dictionary.Matched.Terms* property

Data Loss Prevention rule set

The Data Loss Prevention (DLP) rule set is a library rule set for preventing sensitive content from leaving your network or inappropriate content from entering it.

Default rule set – Data Loss Prevention (DLP)
Criteria – *Always*
Cycles – Requests (and IM), responses, embedded objects

The following rule sets are nested in this rule set:

- DLP in Request Cycle
- DLP in Response Cycle

  This rule set is not enabled by default.

DLP in Request Cycle

This nested rule set blocks requests that are sent from clients of our network to web servers if it is detected that sensitive content is involved. For example, a request to upload a file to the web that has sensitive content is blocked.

Nested library rule set – DLP in Request Cycle
Criteria – *Cycle.TopName equals "Request"*
Cycles – Requests (and IM) and embedded objects

The rule set criteria specifies that the rule set applies when a request is processed on the appliance.

The rule set contains the following rules:

Block files with HIPAA information

DLP.Classification.BodyText.Matched <HIPAA> equals true –> Block<DLP.Classification.Block> – Statistics.Counter.Increment (“BlockedByDLPMatch”,1)<Default>

The rule uses the *DLP.Classification.BodyText.Matched* property to check whether the body of the request that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that uploading to the web is requested for.

Text is considered to be sensitive content according to the HIPAA health care regulations. Use of the relevant information is configured as part of the module settings, which are specified after the property name.

If there is sensitive content in the text of a request body, the request is blocked. The settings of the Block action specify a message to the requesting user.

The rule also uses an event to count blocking due to a data loss prevention match.

Block files with Payment Card Industry information

DLP.Classification.BodyText.Matched <Payment Card Industry> equals true –> Block<DLP.Classification.Block> – Statistics.Counter.Increment (“BlockedByDLPMatch”,1)<Default>

The rule uses the *DLP.Classification.BodyText.Matched* property to check whether the body of the request that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that uploading to the web is requested for.

Text is considered to be sensitive content according to the regulations that apply for payment cards. A credit card number would, for example, be content under these regulations. Whether there is sensitive content in a text, is detected using appropriate information in the same way as for the HIPAA-related rule.

If there is sensitive content in the text of a request body, the request is blocked. The settings of the Block action specify a message to the requesting user.

The rule also uses an event to count blocking due to a data loss prevention match.

Block files with SOX information

DLP.Classification.BodyText.Matched <SOX> equals true –> Block<DLP.Classification.Block> – Statistics.Counter.Increment (“BlockedByDLPMatch”,1)<Default>

The rule uses the *DLP.Classification.BodyText.Matched* property to check whether the body of the request that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that uploading to the web is requested for.

Text is considered to be sensitive content according to the regulations of the Sorbanes-Oxley (SOX) act on public company accountability. Board meeting minutes would, for example, be sensitive content under this act. Whether there is sensitive content in a text, is detected using appropriate information in the same way as for the HIPAA-related rule.

If there is sensitive content in the text of a request body, the request is blocked. The settings of the Block action specify a message to the requesting user.

The rule also uses an event to count blocking due to a data loss prevention match.

DLP Response Cycle

This nested rule set blocks responses that are received on the appliance from web servers if it is detected that they contain inappropriate content, for example, discriminatory or offensive language.

Nested library rule set – DLP Response Cycle
Criteria – *Cycle.TopName equals "Response"*
Cycles – Reponses and embedded objects

The rule set criteria specifies that the rule set applies when a response is processed on the appliance.

The rule set contains the following rule:

Acceptable use

DLP.Classification.BodyText.Matched <Acceptable Use> equals true –>
Block<DLP.Classification.Block> – Statistics.Counter.Increment ("BlockedByDLPMatch",1)<Default>

The rule uses the *DLP.Classification.BodyText.Matched* property to check whether the body of the response that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that is sent in response to a download request.

The module that Is called by the rule to find out whether there is inapproriate content in the response body uses appropriate information from classification lists. Use of these lists is configured as part of the module settings, which are specified after the property name.

If there is inappropriate content in the text of a response body, the response is blocked. The settings of the Block action specify a message to the user who the response should have forwarded to.

The rule also uses an event to count blocking due to a data loss prevention match.

Preventing data loss using an ICAP server

When you have implemented data loss prevention with an ICAP server that handles the filtering process, you can configure settings and implement a rule set to ensure the smooth flow of data between the appliance and the ICAP server.

You can use a solution called nDLP for data loss prevention. Within this solution, data that users want to upload from your network to the web is filtered to prevent data loss. The filtering is done on an ICAP server. The data flow is as follows:

- Data sent from the client systems of your users is forwarded to the appliance.
- The appliance provides an ICAP client that sends REQMOD requests with the user data to the ICAP server.
- The requests are filtered on the server by modifying them according to the ICAP protocol and passed on to the web servers that are the destinations of the requests.

After importing the *Data Loss Prevention with ICAP* rule set from the library, rules that are implemented on the appliance control the sending of requests to the ICAP server.

According to these rules, a request is not forwarded if:

- The body of the request contains no data and the request does not include URL parameters.
- The body of the request exceeds a given size (default: 50 MB).

Together with the rule set, settings are imported that you need to configure. These include a list of the ICAP servers that the appliance can forward requests to.

You can also configure the ICAP client on the appliance not to open more connections for sending requests than a particular ICAP server can handle at the same time.

Create an ICAP server list for data loss prevention

When running the nDLP solution for data loss prevention, which uses an ICAP server for filtering data, you need to configure a list of these servers.

Task

1. Select **Policy** | **Settings**.
2. On the settings tree, select **ICAP Client** and click the **ReqMod** settings.
3. Configure the the ICAP server list that is provided under these settings as needed.
4. Click **Save Changes**.

ICAP Client settings

The ICAP Client settings are used for configuring communication in REQMOD mode between an ICAP client on the appliance and ICAP servers.

ICAP Service

Settings for ICAP servers that the ICAP client on the appliance sends requests to

Table 10-28 Select Scanning Engines

Option	Definition
List of ICAP Servers	List of server lists for the ICAP communication

The following table describes an entry for an ICAP server in a server list.

Table 10-29 Entry in a list of ICAP servers

Option	Definition
URI	URI of an ICAP server Format: ICAP://<IP address>:<port number>
Respect max concurrent connections limit	When selected, the ICAP client on the appliance will not open more connections at the same time for sending requests than the ICAP server can handle.
Comment	Plain-text comment on the ICAP server

Data Loss Prevention With ICAP rule set

The Data Loss Prevention with ICAP rule set is a library rule set for configuring the data flow between the appliance and an ICAP server in a solution for data loss prevention.

Library rule set – Data Loss Prevention With ICAP
Criteria – *Criteria — URL.Host does not equal " "*
Cycles – Requests (and IM) and embedded objects

The rule set criteria specifies that the rule set applies when a host name can be found for a URL that is sent in a request to the appliance.

The rule set contains the following rules.

Skip requests that do not carry information

Body.Size equals 0 AND ListOfString.IsEmpty(URL.Parameters) equals true –> Stop Rule Set

The rule uses the *Body.Size* property to check whether a request has a body that is empty. It also uses the *ListOfString.IsEmpty* property to check whether a request has URL parameters.

If one of the two parts of this criteria is matched, processing of the rule set stops and the request is not forwarded to the ICAP server.

Skip body that is greater than 50 MB

Body.Size greater than 50 –> Stop Rule Set

The rule uses the Body.Size property to check whether the body of a request does not exceed 50 MB. If it does, processing of the rule set stops and the request is not forwarded to the ICAP server.

Call ReqMod server

ICAP.ReqMod.Satisfaction<ReqMod> equals true –> Stop Cycle

When a request has passed filtering according to the first two rules of the rule set, it is forwarded to the ICAP server. If this has been done, the value of the ICAP.ReqMod.Satisfaction property is true.

The rule checks whether this is the case for a request and eventually stops processing the current cycle.

11 Supporting functions

Some functions on the appliance do not filter web objects or users, but support the filtering process in different ways.

You can use the supporting functions to do the following:

- **Show download progress** — You can configure methods to show users the progress made in downloading web objects.
- **Throttle bandwith for uploads and downloads** — You can limit the speed for uploading data from clients to the appliance or downloading them from web servers to the appliance.
- **Use the web cache to store and provide web objects** — You can speed up responses to client requests by delivering objects from the web cache on the appliance.
- **Route requests through next-hop proxies** — You can use these proxies to route requests to their destination.

Contents

Progress indication

Progress indication is a process that shows a user who has started the download of a web object the progress made in downloading the object.

The following elements are involved in this process:

- Progress indication rules that control the process
- Progress indication modules that are called by the rules to handle the different methods for progress indication

Progress indication rules

The rules that control progress indication are usually contained in one rule set. Different rules control the use of different methods for progress indication. Accordingly, they call different modules to handle these methods.

Two methods for progress indication are available on the appliance. Which method is appropriate for a download depends on the browser that a user sends the download request with.

- **Progress page** — For Mozilla browsers

  Under this method, a page with a progress bar is shown to the user who started a download and then another page for download completion.

- **Data trickling** — For all other browsers

  Under this method, a web object is forwarded to the user in chunks and at a particular forwarding rate.

Progress indication is not implemented with the default rule set system. A library rule set provides these functions. It's name is *Progress Indication*.

You can implement this rule set, review its rules, modify or delete them, and also create your own rules.

Progress indication modules

Two progress indication modules (also known as *engines*) are available for handling different methods of progress indication:

- **Progress Page module** — For the progress page method
- **Data Trickling module** — For the data trickling method

You can configure settings for these modules to modify the way they handle these methods.

Templates are provided for configuring the two pages used for the progress page method. The configuration is done in the same way as for user message templates.

Configure progress indication

You can implement progress indication and configure it to adapt it to the needs of your network.

Complete the following high-level steps.

Task

1. Import the Progress Indication rule set from the library.
2. Review the rules in this rule set and modify them as needed.

   You can, for example, do the following:

   - Configure settings for the Progress Page module:
     - Choose a particular language for the progress page
     - Modify the text of the progress page
     - Specify timeouts for the downloaded page, for example, a timeout for the time that a page is available after the download
   - Configure settings for the Data Trickling module:
     - Size of the first chunk in the trickling process
     - Forwarding rate
3. Save your changes.

Configure the progress indication modules

You can configure the progress indication modules to modify the way progress made in downloading a web objects is shown to users.

There are two different modules for progress indication: the Progress Page and the Data Trickling modules.

Task

1 Select **Policy Rule Sets**.

2 On the rule sets tree, select the rule set for progress indication.

If you have implemented the library rule set for this function, this is the *Progress Indication* rule set.

The rules of the rule set appear on the settings pane.

3 Make sure **Show details** is selected.

4 Find the rule that calls the Progress Page module or the rule that calls the Data Trickling module, according to what you want to configure.

In the library rule set, these are the rules *Enable progress page* and *Enable data trickling*.

5 In the rule event of the appropriate rule, click the settings name.

The **Edit Settings** window opens. It provides the settings for the Progress Page or the Data Trickling module.

6 Configure these settings as needed.

7 Click **OK** to close the window.

8 Click **Save Changes**.

See also

Progress Page settings on page 249
Data Trickling settings on page 250

Progress Page settings

The Progress Page settings are used for configuring the progress page that is shown to users when they are downloading web objects.

Progress Page Parameters

Settings for the progress page

Table 11-1 Progress Page Parameters

Option	Definition
Templates	Settings for the templates used by the progress page
Timeouts	Settings for the timeouts that are related to the progress page

Templates

Settings for the templates used by the progress page

Table 11-2 Templates

Option	Definition
Language	Settings for selecting the language of the progress page • **Auto (Browser)** — When selected, the message is in the language of the browser that the blocked request was sent from • **Force to** — When selected, the message is in the language chosen from the list that is provided here • **Value of 'Message.Language' property** — When selected, the message is in the language that is the value of the Message.Language property This property can be used for creating a rule.
Collection	List for selecting a template collection • **Add** — Opens the Add Template Collection window for adding a template collection • **Edit** — Opens the Template Editor for editing a template collection
Template name for progress bar page	List for selecting a template • **Add** — Opens the Add Template window for adding a template • **Edit** — Opens the Template Editor for editing a template
Template name for download finished page	List for selecting a template • **Add** — Opens the Add Template window for adding a template • **Edit** — Opens the Template Editor for editing a template
Template name for download canceled page	List for selecting a template • **Add** — Opens the Add Template window for adding a template • **Edit** — Opens the Template Editor for editing a template

Timeouts

Settings for the timeouts that are related to the progress page

Table 11-3 Templates

Option	Definition
Delay for redirects to progress page	Time (in seconds) to elapse before the progress page appears
File availability time before download	Time (in minutes) to elapse before a file is no longer available to a user before the download
File availability time after download	Time (in minutes) to elapse before a file is no longer available to a user after the download

Data Trickling settings

The Data Trickling settings are used for configuring the data trickling process that is applied when a user has started the download of a web object.

Data Trickling Parameters

Settings for the portions of a web object that are forwarded in data trickling mode

Table 11-4 Data Trickling Parameters

Option	Definition
Size of first chunk	Size (in bytes) of the first chunk of a web object that is forwarded using the data trickling method
Forwarding rate	Portion of a web object that is forwarded every five seconds The forwarding rate is the thousandth part of the entire volume that is to be forwarded multiplied by the value you configure here.

Progress Indication rule set

The Progress Indication rule set is a library rule set for showing users the progress made in downloading a web object.

Library rule set – Progress Indication
Criteria – *MediaType.FromHeader does not equal text/htm*
Cycles – Requests (and IM), responses, embedded objects

The rule set criteria specifies that the rule set applies when media that is sent from the web in response to the request submitted by a user not of the text or htm type.

The rule set contains the following rules.

Progress Page

*Header.Request.Get ("User-Agent") matches *(Mm)ozilla** –> Stop Rule Set – Enable Progress Page <Default>

The rule enables a progress page for Mozilla browsers. The event settings specify what the progress page looks like, for example, the language it uses.

Data Trickling

Always –> Stop Rule Set – Enable Data Trickling<Default>

The rule enables data trickling for all browsers that are not Mozilla. The event settings specify the chunk and block sizes used for the trickling.

Bandwidth throttling

You can limit the speed for uploading and downloading data to the appliance in a process also known as *bandwidth throttling*.

You can use bandwidth throttling, for example, to avoid a situation where the network performance you need for completing a particular task is impacted by other users who are individually uploading objects to the web or are requesting large downloads from the web.

Bandwidth throttling rules

Bandwidth throttling rules limit the transferring speed when user upload objects to the web or download them.

Events in bandwidth throttling rules

Two events are available for use in rules that control bandwidth throttling:

- **Throttle.Client** — Limits the speed of data transfer from a client to the appliance

  This is the case when a client sends a request for uploading an object to a web server and the request is intercepted on the appliance together with the object.

- **Throttle.Server** — Limits the speed of data transfer from a web server to the appliance

  In this case, there has been a client request to download an object from a web server, and after this request has been filtered on the appliance and forwarded, the web server sends the object in response.

Bandwith throttling rule for uploads

The following is an example of a rule that can execute bandwidth throttling rule for uploads.

Limit upload speed for hosts on throttling list

URL.Host is in list Upload Throttling List –> Continue – Throttle.Client (10)

The rule uses the *Throttle.Client* event to limit the speed with which uploads are performed to 10 Kbps if the web server that the data should be uploaded to is on a particular list.

In the criteria of the rule, the URL.Host property is used to retrieve the host name of the web server that is specified in the uploading request.

If the Upload Throttling List contains this name, the criteria is matched and the rule applies. The throttling event is then executed.

The Continue action lets rule processing continue with the next rule.

Bandwith throttling rule for downloads

The following is an example of a rule that can execute bandwidth throttling rule for downloads.

Limit download speed for media types on throttling list

MediaType.EnsuredTypes at least one in list MediaType Throttling List –> Continue – Throttle.Server (1000)

The rule uses the *Throttle.Server* event to limit the speed with which downloads are performed to 1000 Kbps if the web object that should be downloaded belongs to a media type on a particular list.

In the criteria of the rule, the MediaType.EnsuredTypes property is used to detect the media type of the web object that the web server sends. An object can also be found to belong to more than one type.

If any of these types is on the Media Type Throttling List, the criteria is matched and the rule applies. The throttling event is then executed.

The Continue action lets rule processing continue with the next rule.

Bandwidth throttling rules and rule sets

We recommend that you create an overall rule set for bandwidth throttling rules and embed two rule sets in it, one for throttling uploads and another for throttling downloads. You can then let the embedded upload rule set apply for the request cycle and the embedded download rule set for the response cycle.

Within each embedded rule set, you can have multiple throttling rules that apply to different kinds of web objects.

The overall rule set for bandwidth throttling should be placed at the beginning of your rule set system. If this is not done, rules in other rule sets can start unthrottled downloads of web objects before your throttling rules are executed.

For example, a rule for virus and malware filtering could trigger the download of a web object that has been sent by a web server in response to a user request. The web object then needs to be completely downloaded to the appliance to see whether it is infected.

If your bandwidth throttling rule set is placed and processed after the rule set with the virus and malware filtering rule, bandwidth throttling is not applied to that download.

Configure bandwidth throttling

You can implement bandwidth throttling and configure it to adapt it to the needs of your network.

Complete the following high-level steps.

Task

1. Create lists of web objects for use by the bandwidth throttling rules.

   You can, for example, create the following:

   - A list of hosts that transferring speed is limited for when objects are uploaded to them
   - A list of media types that transferring speed is limited for when they an object that belongs to one of these types is downloaded

2. Create a rule set for bandwidth throttling.

3. Within this rule set, create rules for bandwidth throttling.

   You can, for example, create the following:

   - A rule for limiting transferring speed when objects are uploaded to particular hosts.
   - A rule for limiting transferring speed when an object that belongs to a particular media type is downloaded.

4. Design these rules as needed.

   You can, for example, do the following:

   - Configure a particular transferring speed for the *Throttle.Client* event that enables bandwidth throttling for uploading objects to the web.
   - Configure a particular transferring speed for the *Throttle.Server* event that enables bandwidth throttling for downloading objects from the web.

5. Save your changes.

Web caching

A web cache is provided on the appliance for storing web objects to speed up responses to client requests.

Use of the appliance web cache is controlled by rules in a rule set.

To find out whether a web cache rule set is implemented on your appliance, review the system of rule sets on the **Rule Sets** tab of the **Policy top-level** menu.

If none is implemented, you can import the Web Cache library rule set. After importing this rule set, you can review and modify it on the **Rule Sets** tab to make it suit your network. Alternatively, you can create a rule set with rules of your own.

A web cache rule set typically contains rules for reading objects from the cache and writing them to it.

Additionally, there can be bypass rules that exclude objects from being read or written.

Verify the enabling of the web cache

You can verify whether the web cache is enabled.

Task

1. Select **Configuration Appliances**.
2. On the appliances tree, select the appliance that you want to verify enabling of the web cache for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.
3. Scroll down to the **Web Cache** section and see whether **Enable Cache** is selected. If necessary, enable this option.
4. If necessary, click **Save Changes**.

See also

Proxies settings on page 118

Web Cache rule set

The Web Cache rule set is a library rule set for web caching.

Library rule set – Web Cache
Criteria – *Always*
Cycles – Requests (and IM) and responses

The following rule sets are nested in this rule set:

- Read from Cache
- Write to Cache

Read from Cache

This nested rule set enables the reading of web objects from the cache and forbids it for URLs that are on a bypassing list.

Nested library rule set – Read from Cache
Criteria – *Always*
Cycles – Requests (and IM)

The rule set contains the following rules.

Skip caching URLs that are in Web Cache URL Bypass List

URL matches in list Web Cache URL Bypass List –> Stop Rule Set

The rule uses the *URL property* to check for requested URLs whether they are on the specified bypass list.

If they are, processing of the rule set stops. The rule that enables reading from the cache is then not processed.

Processing continues with the next rule set.

The rule is not enabled by default.

Enable Web Cache

Always –> Continue — Enable Web Cache

The rule is always processed unless it is skipped because the bypassing rule placed before it in the rule set applies. It enables the web cache, so objects stored in it can be read.

Processing continues with the next rule set.

Write to Cache

This nested rule set enables the writing of web objects to the cache and forbids it for large objects, as well as for URLs and media types on particular bypassing lists.

Nested library rule set – Write to Cache
Criteria – *Always*
Cycles – Responses

The rule set contains the following rules.

Skip caching URLs that are in Web Cache URL Bypass List

URL matches in list Web Cache URL Bypass List –> Stop Rule Set

The rule uses the *URL property* to check for requested URLs whether they are on the specified bypass list.

If they are, processing of the rule set stops. The rule that enables reading from the cache is then not processed.

Processing continues with the next rule set.

The rule is not enabled by default.

Skip caching URLs that are in Web Cache URL Bypass List

URL matches in list Web Cache URL Bypass List –> Stop Rule Set

The rule uses the *URL property* to check for requested URLs whether they are on the specified bypass list.

If they are, processing of the rule set stops. The rule that enables reading from the cache is then not processed.

Processing continues with the next rule set.

The rule is not enabled by default.

Skip caching URLs that are in Web Cache URL Bypass List

URL matches in list Web Cache URL Bypass List –> Stop Rule Set

The rule uses the *URL property* to check for requested URLs whether they are on the specified bypass list.

If they are, processing of the rule set stops. The rule that enables reading from the cache is then not processed.

Processing continues with the next rule set.

The rule is not enabled by default.

Enable Web Cache

Always –> Continue — Enable Web Cache

The rule is always processed unless it is skipped because the bypassing rule placed before it in the rule set applies. It enables the web cache, so objects stored in it can be read.

Processing continues with the next rule set.

Next-hop proxies

Next-hop proxies can be used for routing requests received from clients of the appliance to their destinations.

When next-hop proxies are implemented, rules in a corresponding rule set use a module (alson known as *engine*) to call proxies that have been entered onto a list for routing requests.

For example, you can route requests that have internal destinations using internal proxies. IP addresses of destinations that are internal are then entered onto a list, which the routing rule relies on. Similarly, there can be a list of internal next-hop proxy servers for use by the rule.

A rule set with rules for using next-hop proxies is not implemented on the appliance after the initial setup. You can import a rule set from the library and modify it according to your needs or create a rule set of your own.

When you import a next-hop proxy rule set, a server list is also imported, which is initially empty and must be filled by you. You can also create more than one list and use these lists for routing in different situations.

Settings for the next-hop proxy module are imported with a library rule set as well. You can configure these settings to let the module use a particular next-hop proxy list and to determine the mode of calling the proxies (round-robin or failover).

Next-hop proxy modes

When multiple servers are available as next-hop proxies for routing requests, the next-hop proxy module can use two modes to call them: round-robin and failover.

When routing a request in round-robin mode, the next-hop proxy module calls the server that is next on the list to the one that was called last time.

For the next request, this is handled in the same way, so all servers on the list will eventually have been used as next-hop proxies.

The following diagram shows a next-hop proxy configuration in round-robin mode.

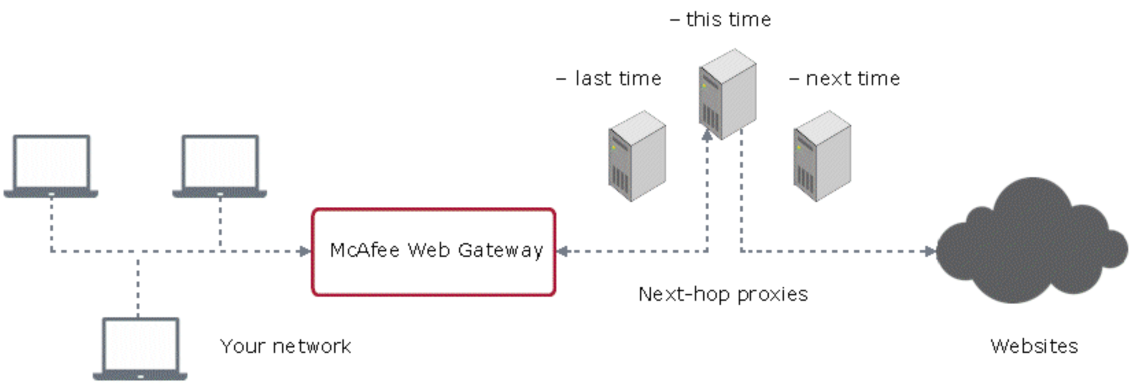


Figure 11-1 Next-hop proxies in round-robin mode

When routing a request in failover mode, the next-hop proxy module calls the first server on the list.

If the server fails to respond, the call is repeated until the configured number of retries is reached. Only then is the next server in the list tried. It is called in the same way as the first, and eventually the next server in the list is tried. This is continued until a server responds or all servers in the list were found to be unavailable.

The following diagram shows a next-hop proxy configuration in failover mode.

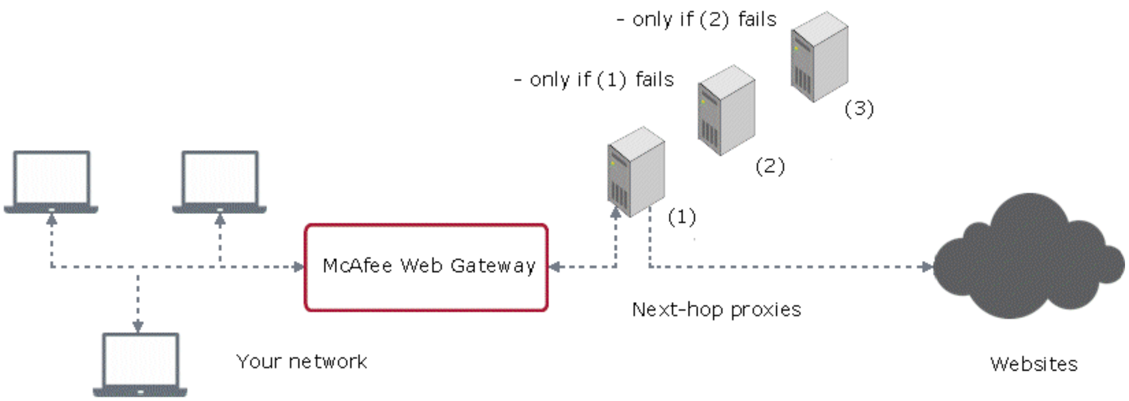


Figure 11-2 Next-hop proxies in failover mode

Configure next-hop proxies

You can implement the use of next-hop proxies and configure it to adapt it to the needs of your network.

Complete the following high-level steps.

Task

1 Import the Next Hop Proxy rule set from the library.

2 Review the rules in this rule set and modify them as needed.

You can, for example, do the following:

- Edit the lists used by the next-hop proxy rule.

  > A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

- Configure the settings of the Next Hop Proxy module

3 Save your changes.

Configure the Next Hop Proxy module

You can configure the Next Hop Proxy module to modify the way next-hop proxies are used for forwarding requests to the web.

Task

1 Select **Policy** | **Rule Sets**.

2 On the rule sets tree, select the rule set for next-hop proxies.

If you have implemented the library rule set for this function, this is the *Next Hop Proxy* rule set.

The rules of the rule set appear on the settings pane.

3 Make sure **Show details** is selected.

4 Find the rule that calls the Next Hop Proxy module.

In the library rule set, this is the rule *Use internal proxy for internal host*.

5 In the rule event, click the settings name.

In the library rule set, this name is *Internal Proxy* .

The **Edit Settings** window opens. It provides the settings for the Next Hop Proxy module.

6 Configure these settings as needed.

7 Click **OK** to close the window.

8 Click **Save Changes**.

See also
Next Hop Proxy settings on page 258

Next Hop Proxy settings

The Next Hop Proxy settings are used for configuring next-hop proxies to forward requests that have been received on the appliance to the web.

Next Hop Proxy Server

Settings for next-hop proxies

Table 11-5 Next Hop Proxy Server

Option	Definition
List of next-hop proxy servers	List for selecting a next-hop proxy server list
Round robin	When selected, the Next Hop Proxy module uses the next-hop proxy following the one in the list that has been used last. When the end of the list has been reached, the first next-hop proxy in the list is again selected.
Fail over	When selected, the Next Hop Proxy module tries the first next-hop proxy in the list first. If it fails, it is retried until the configured retry maximum has been reached. Then the second next-hop proxy in the list is tried, and so on, until a server responds or all are found to be unavailable.

Next Hop Proxy rule set

The Next Hop Proxy rule set is a library rule set for using next-hop proxies to forward requests to the appropriate web servers.

Library rule set – Next Hop Proxy
Criteria – *Always*
Cycle – Requests (and IM)

The rule set contains the following rule.

Use internal proxy for internal host

URL.Destination.IP is in range list Next Hop Proxy IP Range List OR

URL.Destination.IP is in list Next Hop Proxy IP List –> Continue — Enable Next Hop Proxy<Internal Proxy>

The rule uses the *URL.Destination.IP* property to check whether an IP address that corresponds to a URL is in one of the ranges specified on a list or is on a list directly. If it is, the rule uses an event to route requests for access to these URLs through internal next-hop proxies.

The event settings specify settings that include the next-hop proxy list and the mode for calling proxies.

12 User messages

Messages can be sent to users when a filtering rule blocks their requests for web access or affects them in other ways.

When you are administering this process, you are mainly dealing with the following:

- **Messages** — Messages are sent to users to inform them that their requests for web access are blocked, or redirected, or that they need to authenticate.
- **Action settings** — Messages to users are part of the settings for the action that is explained in a message.
- **Templates** — Messages to users are based on templates, which can be edited using the Template Editor.

Default settings apply for user messages and their templates after the initial setup of the appliance, which you can review and modify as needed.

Contents

Sending messages to users

Messages are sent to users to inform them about actions of the filtering rules that affect them.

User messages belong to different types and are based on templates.

Message types

There are different types of user messages, according to the action that a message informs a user about.

- **Authenticate message** — Informs a user that authentication is required to access a URL
- **Block message** — Informs a user that a request was blocked for various reasons, for example, because a virus was detected in the requested object
- **Redirect message** — Informs a user that redirecting to another URL is needed for accessing the requested object

Message templates

Messages that are sent to users are based on templates. To modify what a message looks like, you need to adapt these templates. You can do this under the settings for an action.

Message templates contain standard text with variables. The variables are filled with values as needed in a given situation.

All variables used in message templates are also properties used by rules. For example, *URL* is a variable in a message text and a property when used in a rule to exempt URLs from filtering.

Message text and variables

The following text and variables could be contained in a Block message that is sent to a user when access to a requested object has been block due to a virus infection of the object.

- **Standard text** — *The transferred file contained a virus and was therefore blocked.*
- **Variables** — as follows:
  - **URL** — URL that the user requested to access the file

    The variable used to display a URL is *$URL$*.
  - **Virus name** — Name of the found virus that caused the blocking of the file

    The variable used to display a virus name is *$List.OfString.ByName(String)$*.

    When editing a message template, you can select and insert variables from a list of properties. To serve as variables in message templates, these are converted into strings (if they are not strings already).

    For this reason, it makes no sense to select “string converter” properties here, which are properties whose job it is to convert other data types into strings, for example, the NumberToString(String) property.

Template versions and collections

Different versions can exist of a particular template regarding:

- **File format** — *.html* or *.txt*
- **Language** — Language of template

You can group templates into collections and have, for example, a default collection and collections for other purposes.

Template Editor

The Template Editor is a device on the user interface that allows you to edit existing templates for user messages.

You can access it when configuring the settings of an action that affects the user, for example, of the Block action.

When editing a message template, you can do the following:

- Select a language for the message
- Edit the message text
- Replace the variables in the template
- Specify a block reason for logging purposes (only for Block action templates)
- Specify a URL for redirecting (only for Redirect action templates)

Edit the text of a user message

You can edit the text of a user message to adapt it to the requirements of your network.

Task

1 Select **Policy | Rule Sets**.

2 Select the rule set of a rule that includes the action with the user message you want to edit.

For example, select the **Gateway Antimalware** rule set.

The rules of the rule set appear on the settings pane.

3 Make sure **Show Details** is enabled.

4 In the appropriate rule, click the settings of the action with the user message.

For example, in the rule **Block if virus was found**, click the **Virus Found** settings of the Block action.

The **Edit Settings** window opens.

5 Next to the **Template Name** field, click **Edit**.

The Template Editor opens.

6 On the templates tree, expand the appropriate action template folder, for example, **Virus Found**.

The available language versions of the template appear.

7 Expand a language version, for example, **en** for English.

The available message formats of the language version appear.

8 Select a format, for example, **html**.

The content of the template appears on the settings pane in the selected format. It contains the text of the user message.

For example, in the HTML format of the English **Virus Found** template, this text reads initially:

The transferred file contained a virus and was therefore blocked.

9 Edit the text as needed.

10 Click **Save Template Changes**.

The Template Editor closes.

11 Click **OK** to close the **Edit Settings** window.

See also

Template Editor on page 266

Authenticate settings

The *Authenticate* settings are used for configuring the way the Authenticate action is executed when a filtering rule with that action applies.

Failed Login Message Template

Settings for configuring user messages and a block reason for logging purposes

Table 12-1 Failed Login Message Template

Option	Definition
Language	Settings for selecting the language of a user message • **Auto (Browser)** — When selected, the message is in the language of the browser that the blocked request was sent from • **Force to** — When selected, the message is in the language chosen from the list that is provided here • **Value of Message.Language property** — When selected, the message is in the language that is the value of the *Message.Language* property This property can be used for creating a rule.
Template collection	List for selecting a template collection • **Add** — Opens the **Add Template Collection** window for adding a template collection • **Edit** — Opens the Template Editor for editing a template collection
Template name	List for selecting a template • **Add** — Opens the *Add Template* window for adding a template • **Edit** — Opens the Template Editor for editing a template
McAfee Web Reporter block reason ID	Numerical value for a block reason
Block reason	Block reason in plain text

Block settings

The Block settings are the used for configuring the way the Block action is executed when a filtering rule with that action applies.

Language and Template Settings

Settings for configuring user messages and a block reason for logging purposes

Table 12-2 Language and Template Settings

Option	Definition
Language	Settings for selecting the language of a user message • **Auto (Browser)** — When selected, the message is in the language of the browser that the blocked request was sent from • **Force to** — When selected, the message is in the language chosen from the list that is provided here • **Value of Message.Language property** — When selected, the message is in the language that is the value of the *Message.Language* property This property can be used for creating a rule.
Template collection	List for selecting a template collection • **Add** — Opens the **Add Template Collection** window for adding a template collection • **Edit** — Opens the Template Editor for editing a template collection

Table 12-2 Language and Template Settings *(continued)*

Option	Definition
Template name	List for selecting a template • **Add** — Opens the **Add Template** window for adding a template • **Edit** — Opens the Template Editor for editing a template
McAfee Web Reporter block reason ID	Numerical value for a block reason
Block reason	Block reason in plain text

Redirect settings

The *Redirect* settings are used for configuring the way the Redirect action is executed when a filtering rule with that action applies.

Redirect Settings

Settings for configuring user messages and a block reason for logging purposes

Table 12-3 Redirect Settings

Option	Definition
Redirect.URL	When selected, the value of the *Redirect.URL* property is the URL that is used for redirecting. This property can be used in a suitable rule.
User-defined URL	When selected, the redirecting URL must be specified by you
Redirect URL	Input field for the redirecting URL
Language	Settings for selecting the language of a user message • **Auto (Browser)** — When selected, the message is in the language of the browser that the blocked request was sent from • **Force to** — When selected, the message is in the language chosen from the list that is provided here • **Value of Message.Language property** — When selected, the message is in the language that is the value of the *Message.Language* property This property can be used for creating a rule.
Template collection	List for selecting a template collection • **Add** — Opens the **Add Template Collection** window for adding a template collection • **Edit** — Opens the Template Editor for editing a template collection
Template name	List for selecting a template • **Add** — Opens the **Add Template** window for adding a template • **Edit** — Opens the Template Editor for editing a template
McAfee Web Reporter block reason ID	Numerical value for a block reason
Block reason	Block reason in plain text

Template Editor

The Template Editor is a device on the user interface that allows you to edit existing templates for user messages.

Templates

Provides a tree structure for viewing templates and selecting them for editing.

The following table describes the *Templates* options.

Table 12-4 Templates

Option	Definition
Template collections	Collections of templates, for example, the *Default* collection
Templates	Templates belonging to a collection, for example, the *Virus Found* template For each template, the following is provided under a tree node: • **de, en ...** — Language versions of the template • **html** — version in *.html* format • **txt** — version in *.txt* format When you select a format, the template content appears on the *HTML Editor* pane.
Import	Opens the **Import** window to let you browse to a file containing html and txt template versions for a particular language and import it.
Export	Opens the **Export** window to let you browse to a template file and export it.
Expand All	Expands all collapsed items on the templates tree.
Collapse All	Lets all expanded items collapse.
Right-click on a collection, template, language version, or format	Opens a menu with the following options. The selection of the options varies with the item that the right-click is performed on. • **Clone** — Opens the Clone <item> window for inserting a copy of an item under a new name into a collection • **Add Content File** — Opens the Add Content File window for adding a file • **Rename** — Opens the Rename <item> window for renaming an item • **Change** — Opens the Change Language window for changing a language version • **Delete** — Deletes an item A window opens to let you confirm the deletion.

File System

Provides a tree structure for completing general tasks, such as adding, renaming, and deleting template files.

The following table describes the *File System* options.

Table 12-5 File System

Option	Definition
Template collections	Collections of templates, for example, the *Default* collection
Language versions	Templates sorted by language versions and within a language version group first by names, then by formats For example, the *en* (English) language group contains: • *authenticationrequired.html* • *authenticationrequired.txt* • *AuthorizedOnly.html* • *AuthorizedOnly.txt* • and others When you select a format, the template content appears on the *HTML Editor* pane
Images	Image files, with images used in templates, sorted by name
Add	Opens the following menu: • **New File** — Opens the **Filename** window for adding a file with a new name • **New Directory** — Opens the **Rename Directory** window for adding a selected folder of the tree structure under a new name • **Existing File or Directory** — Opens your file manager for selecting and adding a file or folder
Edit	Opens the following menu: • *Rename* — Opens the **Rename <item>** window for renaming an item • **Delete** — Deletes an item A window opens to let you confirm the deletion.
Cut	Copies and deletes a selected item.
Copy	Copies a selected item.
Expand All	Expands all collapsed items on the file system tree.
Collapse All	Lets all expanded items collapse.
A right-click on an item opens a menu with the preceding options. Options that do not apply for an item are grayed out.	

HTML Editor

Displays the content of the template that is currently selected on the **Templates** or **File System** pane for editing.

The following table describes the *HTML Editor* options.

Table 12-6 HTML Editor

Option	Definition
Add	Opens the following menu: • **Resource Reference** — Opens the **Insert Resource Path** window for entering the path to a resource, such as an image or other graphical element, that appears in a template • **Property** — Opens the **Choose Property** window for adding a property that appears as a variable in a template, for example, *$URL$*
Edit	Opens the following menu: • **Cut** — Copies and deletes a selected portion of template content • **Copy** — Copies a selected portion • **Paste** — Pastes a copied portion • **Delete** — Deletes a selected portion • **Select All** — Selects the complete template content
Discard Changes	Undoes your changes in a template.
Show Source	Shows or hides the HTML source code of a template (toggle button).
Languages drop-down menu	Lets you select the language of the preview.
Preview	Shows a preview of a template.

Viewer

Displays the image contained in a currently selected image file.

It is visible (instead of the *HTML Editor*) when an image file is selected on the *File System* tree.

The following table describes the *Viewer* options.

Table 12-7 Viewer

Option	Definition
Zoom In	Enlarges an image.
Zoom Out	Shrinks an image.
Fit to Window	Lets an image fill out the **Viewer** pane.
Original Size	Displays an image in its original size again.

General options

Options for performing general activities when working with the Template Editor

Table 12-8 General options

Option	Definition
Save Template Changes	Saves your changes to a template.
Cancel	Lets you leave the Template Editor without changes.

13 System configuration

The appliance system provides basic functions that are used by other functions, such as web filtering, authentication, or quota management. You can configure this system to adapt it to the requirements of your network.

When configuring the appliance system, you are dealing mainly with:

- **System settings** — Are configured for network interfaces, DNS servers, proxies, Central Management, and other components and methods that are related to the appliance system
- **System files** — Contain settings for functions of the appliance system that can be modified using the File Editor
- **Database updates** — Ensure that relevant information is made available to the filtering functions of an appliance

System configuration is in part performed during the initial setup of an appliance. After this setup, you can complete further configuration activities for the appliance system.

Contents

Initial setup system settings

Performing the initial setup of an appliance includes configuring some of its system settings.

You can leave the initial settings at their default values or implement your own settings. Later on, you can still modify these settings.

The following table shows the settings that are configured at the initial setup and their default values.

Table 13-1 Initial setup system settings

Parameter	Default value
Primary network interface	eth0
Autoconfiguration with DHCP	yes
Host name	mwgappl
Root password	<none>

Table 13-1 Initial setup system settings *(continued)*

Parameter	Default value
Remote root logon with SSH	on
Default gateway	<configured by DHCP>
DNS server	<configured by DHCP>

System configuration after the initial setup

All settings for the appliance system can be configured after its initial setup. This includes the modification of the settings that were configured during this setup.

Settings for the appliance system can be configured in different fields.

System settings for general functions

Some system settings are configured for functions of the appliance system that provide general services, such as licensing or date and time on an appliance.

See also

License settings on page 273
Date and Time settings on page 274
File Server settings on page 275
User Interface settings on page 276

Network system settings

Network system settings are configured to integrate the appliance system into the network.

Some network system settings are already configured at the initial setup, including settings for the primary network interface of an appliance and the DNS server that is used by an appliance.

Later on, you can also configure settings for the proxy functions, port forwarding, static routes, and other network-related functions.

See also

Network settings on page 279
DNS settings on page 280
Network Protection settings on page 281
Port Forwarding settings on page 281
Static Routes settings on page 282
Proxies settings on page 118

Authentication and quota system settings

Authentication and quota system settings are configured to implement methods for authenticating users on an appliance and imposing restrictions on their web usage.

Configuring authentication and quotas is mainly done on an appliance by working with rules in authentication and quota rule sets.

However, a few authentication functions are configured as settings of the appliance system, including settings for the Kerberos authentication method and for Windows domain membership.

Some quota parameters are also configured as system settings.

See also
Kerberos Administration settings on page 149
Windows Domain Membership settings on page 150
Quota system settings on page 189

Web filtering system settings

Web filtering system settings are configured to implement functions for filtering web objects on an appliance.

Web filtering configuration is mainly done on an appliance by working with rules in web filtering rule sets, such as the Gateway Antimalware or the URL Filter rule set.

However, a few web filtering functions are configured as settings of the appliance system, for example, the anti-malware queue, which collects web objects in a queue to limit work load for the scanning modules of an appliance.

See also
Anti-Malware system settings on page 200

Central Management system settings

Central Management system settings are configured when you are running multiple appliances as nodes in a common configuration.

In a Central Management configuration, you can also configure system settings for other nodes from the node you are logged on to.

See also
Central Management settings on page 294

System settings for logging and troubleshooting

System settings for logging and troubleshooting are configured to control the log file manager on an appliance and also for using external components to record log data.

Use of external components includes forwarding data to a McAfee ePO server and monitoring events with an SNMP agent.

See also
Log File Manager settings on page 346
ePolicy Orchestrator settings on page 367
SNMP settings on page 368

Configure the system settings

You can configure settings for the appliance system to adapt it to the requirements of your network.

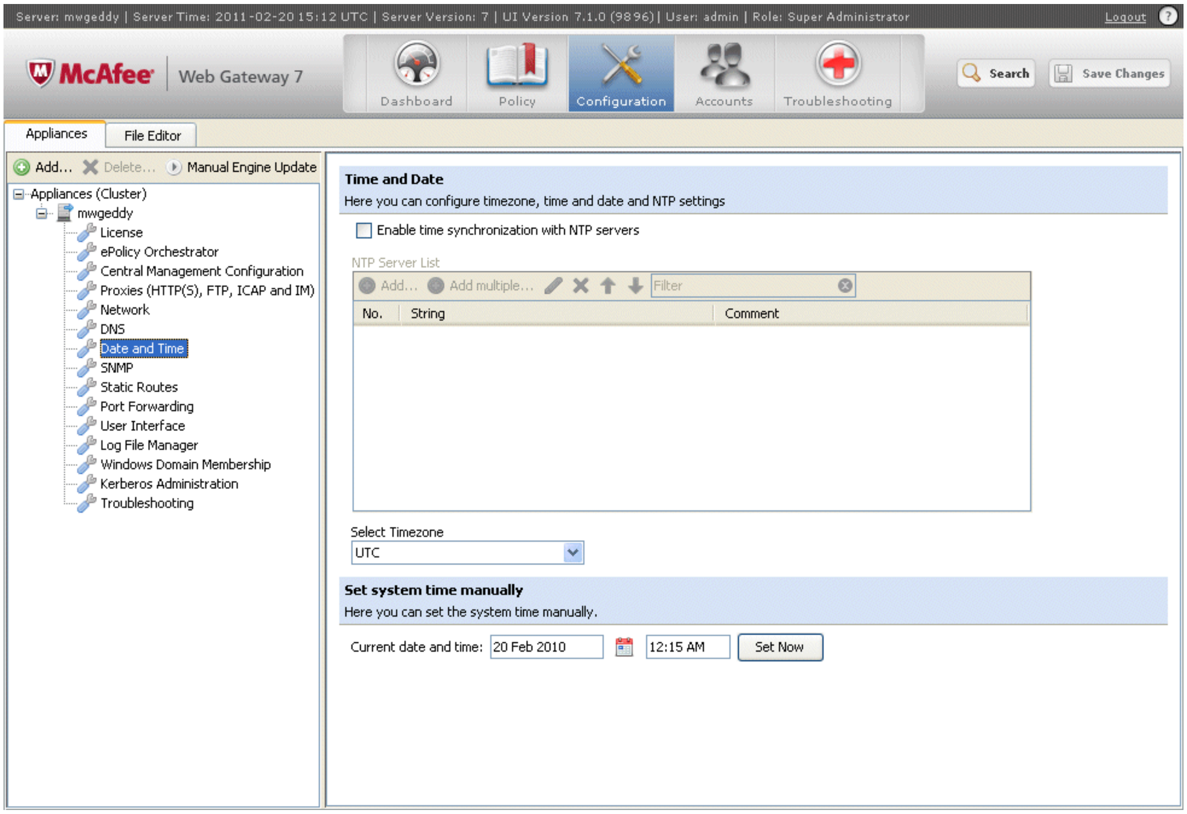
Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select an appliance and click the system settings you want to configure.
3. Configure these settings as needed.
4. Click **Save Changes**.

See also
System configuration after the initial setup on page 270

Appliances tab

The Appliances tab allows you to configure system settings on an appliance.



Server: mwgeddy | Server Time: 2011-02-20 15:12 UTC | Server Version: 7 | UI Version 7.1.0 (9896) | User: admin | Role: Super Administrator

Time and Date

Here you can configure timezone, time and date and NTP settings

□ Enable time synchronization with NTP servers

NTP Server List

No.	String	Comment

Select Timezone: UTC

Set system time manually

Here you can set the system time manually.

Current date and time: 20 Feb 2010 12:15 AM

Main elements of the Appliances tab

The following table describes the main elements of the **Appliances** tab.

Table 13-2 Main elements of the Appliances tab

Element	Description
Appliances toolbar	Toolbar with items for adding appliances to a Central Management configuration, removing them, and updating them all at once
Appliances tree	Tree structure of appliances with the system settings for each appliance
Appliance toolbar (appears when an appliance is selected on the appliances tree)	Toolbar with items for working with a selected appliance
Appliance settings	System settings for the selected appliance

Appliances toolbar

The appliances toolbar provides the following options.

Table 13-3 Appliances toolbar

Option	Definition
Add	Opens the **Add Appliance** window for adding an appliance.
Delete	Deletes a selected appliance. A window opens to let you confirm the deletion.
Manual engine update	Updates DAT files with virus signatures and other filtering information for all appliances in a Central Management configuration.

Appliance toolbar

The appliance toolbar provides the following options.

Table 13-4 Appliance toolbar

Option	Definition
Reboot	Restarts an appliance.
Flush cache	Flushes the web cache of an appliance.
Update appliance software	Installs an updated version of the appliance software.
Shutdown	Lets an appliance become inactive.
Rotate logs	Rotates log files on an appliance.
Rotate and push logs	Rotates log files on an appliance and pushes them to the destination that is specified within the **Log File Manager** settings.

System settings for general appliance functions

Some system settings are configured for functions that provide general services of the appliance system.

Settings for general appliance functions include:

- License settings
- Date and Time settings
- File Server settings
- User Interface settings

License settings

The License settings are used for importing a license to an appliance. Information on the license is shown together with these settings.

License Administration

Settings for importing a license and information on an imported license

Table 13-5 License Administration

Option	Definition
Import License	Items for importing a license - **License file** — Input field for entering the name of a license file You can type a file name here or use the **Browse** button and select an appropriate file. - **Browse** — Opens your local file manager to let you browse to a license file - **Activate** — Activates the license specified in the input field The **Activate** button is grayed out as long as you have not entered a file name in the input field.
License information	Information on an imported license - **Status** — Input field for entering the name of a license file You can type a file name here or use the **Browse** button and select an appropriate file. - **Creation** — Opens your local file manager to let you browse to a license file - **Activate** — Activates the license specified in the input field The **Activate** button is grayed out as long as you have not entered a file name in the input field. - **Expiration** — Date when the license expires - **License ID** — Numerical value that identifies the license - **Customer** — Name of the license owner - **Seats** — Number of workplaces in the owner's company that the license is valid for - **Evaluation** — Information on whether the license has been evaluated

Date and Time settings

The Date and Time settings are used for configuring the time servers that synchronize date and time of the appliance system. They also allow you to set the system time manually.

Date and Time

Settings for date and time of the appliance system

Table 13-6 Date and Time

Option	Definition
Enable time synchronization with NTP servers	When selected, the appliance uses time servers under the NTP (Network Time Protocol) for time synchronization. The system time of the appliance is then synchronized with the time on the NTP servers. This will fail, however, if the delta between both times is too big. We therefore recommend that you restart the appliance after configuring time synchronization with NTP servers. When the appliance restarts, it sets system time to the time on the NTP servers.
NTP server list	List of servers used for time synchronization under the NTP protocol The list elements are as follows: • **String** — Name of an NTP server • **Comment** — Plain-text comment on an NTP server
Select time zone	List for selecting a time zone Time synchronization performed by the NTP servers or manually set time refer to the time zone that you select here

Set System Time Manually

Settings for configuring time and date on the appliance system manually

Table 13-7 Set System Time Manually

Option	Definition
Current date and time	Elements for setting date and time of the appliance system • **Date** — For entering a date by typing it in the field or using a calendar • Calendar icon — Opens a calendar for selecting a date After selecting a date on the calendar and clicking **OK**, the date appears in the date field. • **Time** — For typing a time The system time of an appliance is then synchronized with the time on the NTP servers. This will fail, however, if the delta between both times is too big. We therefore recommend that you restart the appliance after configuring time synchronization with NTP servers. When the appliance restarts, it sets system time to the time on the NTP servers.
Set now	Sets the date and time you have entered into the corresponding fields.

File Server settings

The File Server settings are used for configuring dedicated file server ports on an appliance to enable, for example, the downloading of files by clients.

HTTP Connector Port

Settings for dedicated file server ports on an appliance

Table 13-8 HTTP Connector Port

Option	Definition
Enable dedicated file server port over HTTP	When selected, the dedicated HTTP file server ports configured below are enabled.

HTTP connector	Port number of the dedicated HTTP file server port
	You can enter more than one port number here, separating them by commas. The allowed range is 1024 to 65335.
	You can set up a port forwarding rule if you want to forward requests to ports 1-1023.
	Instead of entering a port number alone, you can enter it with an IP address. This means connecting to an appliance over this port is only allowed when using the specified address.
	For example:
	An appliance has two interfaces with IP addresses as follows:
	`eth0: 192.168.0.10, eth1: 10.149.110.10`
	You enter the following under HTTP connector:
	`4711, 192.168.0.10:4722`
	Then connecting to the appliance over port 4711 is allowed using both IP addresses, whereas connecting over port 4722 requires that IP address 192.168.0.10 is used.
	Restricting connections in the latter way can be used for setting up an intranet.

Enable dedicated file server port over HTTPS	When selected, a dedicated HTTPS file server port is enabled.
HTTPS connector	Port number of the dedicated HTTPS file server port You can enter more than one port number here, separating them by commas. The allowed range is 1024 to 65335. Entering an IP address with a port number can be done in the same way as for the HTTP connector and has the same meaning. You can set up a port forwarding rule if you want to forward requests to ports 1-1023.

User Interface settings

The User Interface settings are used for configuring elements of the user interface, such as ports, the logon page, and a certificate for SSL-secured communication.

HTTP Connector Port

Settings for the ports of the local user interface on an appliance and the session timeout

Table 13-9 HTTP Connector Port

Option	Definition
Enable local user interface over HTTP	When selected, you can connect to the user interface using the HTTP protocol.
HTTP connector	Port for connecting to the user interface under HTTP You can enter more than one port number here, separated by commas. The allowed range is from 1024 to 65335. You can set up a port forwarding rule if you want to forward requests to ports 1-1023. Instead of entering a port number alone, you can enter it with an IP address. This means connecting to the user interface over this port is only allowed when using the specified address.
Enable local user interface over HTTPS	When selected, you can connect to the user interface using the HTTPS protocol.
HTTPS connector	Port for connecting to the user interface under HTTPS You can enter more than one port number here, separating them by commas. The allowed range is from 1024 to 65335. You can set up a port forwarding rule if you want to forward requests to ports 1-1023. Instead of entering a port number alone, you can enter it with an IP address. This means connecting to the user interface over this port is only allowed when using the specified address.
Session timeout	Time (in minutes) to elapse before a session on the user interface is closed if no activities occur The allowed range is from 1 to 9999.

Login Page Options

Settings for the page that is used to log on to the user interface of an appliance

Table 13-10 Login Page Options

Option	Definition
Allow browser to save login credentials	When selected, credentials submitted by a user for logging on to an appliance are saved by the browser.
Restrict browser session to IP address of user	When selected, a session for working with the user interface is only valid as long as the IP address of the client that the user started this session from remains the same.
Let user decide to restrict session for IP address or not	When selected, it is up to the user who started a session for working with the user interface whether it should be valid only for the IP address of the client that the session was started from.
Allow multiple logins per login name	When selected, more than one user can log on to the user interface using the same user name and password.
Use HTTPOnly session cookies (applet loading may take longer)	When selected, HTTPOnly cookies are used for a session with the user interface.

User Interface Certificate

Settings for a certificate that is used in SSL-secured communication over the HTTPS port for the user interface

Table 13-11 User Interface Certificate

Option	Definition
Subject, Issuer, Validity, Extensions	Information on the certificate that is currently in use
Import	Opens the **Import Certificate Authority** window for importing a new certificate.
Certificate chain	Displays a certificate chain that is imported with a certificate.

Import Certificate Authority window

Settings for importing a certificate that is used in SSL-secured communication

Table 13-12 Import Certificate Authority window

Option	Definition
Certificate	Input field for entering the name of a certificate file The file name can be entered manually or by using the **Browse** button in the same line.
Browse	Opens the local file manager to let you browse for and select a certificate file.
Private key	Input field for entering the name of a private key file The file name can be entered manually or by using the **Browse** button in the same line. Only keys that are AES-128-bit encrypted or unencrypted keys can be used here.
Browse	Opens the local file manager to let you browse for and select a private key file.
Password	Input field for entering a password that allows the use of a private key
Import	Opens the **Import Certificate Authority** window for importing a new certificate.
OK	Starts the import process for the specified certificate.
Certificate chain	Input field for entering the name of a certificate chain file The file name can be entered manually or by using the **Browse** button in the same line.
Browse	Opens the local file manager to let you browse for and select a certificate chain file. After importing a certificate with a certificate chain, the certificate chain is displayed in the **Certificate chain** field of the User Interface Certificate settings.

System settings for network functions

Some system settings are configured for functions that integrate the appliance system into your network.

System settings for network functions include proxy settings and the following settings:

- Network settings
- DNS settings
- Network protection settings
- Static Routes settings
- Port Forwarding settings

See also

Proxies settings on page 118

Network settings

The Network settings are used for configuring the network interfaces of an appliance.

Network Interface Settings

Settings for network interfaces

Table 13-13 Network Interface Settings

Option	Definition
Host name	Name of an appliance
Enable these network interfaces	List of network interfaces that can be enabled or disabled
IPv4	Tab for configuring network interfaces under version 4 of the Internet Protocol
IPv6	Tab for configuring network interfaces under version 6 of the Internet Protocol
Advanced	Tab for configuring additional media and a bridge for a network interface

IPv4

Tab for configuring network interfaces under version 4 of the Internet Protocol

Table 13-14 IPv4

Option	Definition
IP settings	List for selecting a method of configuring an IP address for a network interface • **Obtain automatically (DHCP)** — The IP address is automatically obtained, using the Dynamic Network Host Protocol (DHCP). • **Configure manually** — The IP address is configured manually, using the input fields below. If this option is not selected, the input fields are grayed out. • **Disable IPv4** — Version 4 of the Internet Protocol is not used for this interface.
IP address	IP address of a network interface (manually configured)
Subnet mask	Subnet mask of a network interface (manually configured)
Default route	Default route for web traffic using the network interface (manually configured)
MTU	Maximum number of bytes in a single transmission unit
IP aliases	List of aliases for the IP address • **Add alias** — Opens the Input window for adding an alias • **Delete** — Deletes a selected alias

IPv6

Tab for configuring network interfaces under version 6 of the Internet Protocol

Table 13-15 IPv6

Option	Definition
IP settings	List for selecting a method of configuring an IP address for a network interface • **Obtain automatically (DHCP)** — The IP address is automatically obtained, using the Dynamic Network Host Protocol (DHCP). • **Solicit from router** — The IP address is obtained from a router. • **Configure manually** — The IP address is configured manually, using the input fields below. If this option is not selected, the input fields are grayed out. • **Disable IPv6** — Version 6 of the Internet Protocol is not used for this interface.
IP address	IP address of a network interface (manually configured)
Default route	Default route for web traffic using the network interface (manually configured)
MTU	Maximum number of bytes in a single transmission unit
IP aliases	List of aliases for the IP address • **Add alias** — Opens the Input window for adding an alias • **Delete** — Deletes a selected alias

Advanced

Tab for configuring additional media and a bridge for a network interface

Table 13-16 Advanced

Option	Definition
Media	List for selecting additional media for use with a network interface • **Automatically detect** — Media for use with a network interface are automatically detected if available in the network environment of an appliance. • **1000BaseT-FD, 1000Base-HD, ...** — The selected media item is used with a network interface.
Bridge enabled	When selected, web traffic is routed through a network interface in transparent bridge mode. • **Name** — Name of the transparent bridge

DNS settings

The DNS settings are usedr for configuring the domain name servers an appliance connects to for retrieving IP addresses that match the host names submitted in user requests.

Domain Name Service Settings

Settings for the IP addresses of different domain name servers

Table 13-17 Domain Name Service Settings

Option	Definition
Primary domain name server	IP address of the first server
Secondary domain name server	IP address of the second server
Tertiary domain name server	IP address of the third server

Network Protection settings

The Network Protection system settings are used for configuring protective rules for traffic coming in to an appliance from your network.

Network Protection Rules

Settings for configuring network protection rules

Table 13-18 Network Protection Rules

Option	Definition
Enable network protection	When selected, the settings configured in the following for network protection are enabled.
Input policy	List for selecting the action taken on incoming traffic Incoming traffic can either be dropped or accepted.
Allow Ping requests	When selected, the appliance accepts and answers Ping requests.
Exceptions from default policy	List of network devices that send traffic to the appliance system Traffic from these devices is not handled according to the rules that are currently implemented. When these rules drop incoming traffic, traffic sent from the devices listed here is accepted and vice versa.

The following table describes an entry in the list of exceptions from the default policy.

Table 13-19 Exceptions from default policy – list entry

Option	Definition
Device	Name of a network device that sends traffic to the appliance system Typing * or no input means all devices are covered.
Protocol	Protocol used for sending traffic
Source	IP address or address range of the network device or devices that send traffic to the appliance system
Destination port	Port on an appliance that is the destination of network traffic
Comment	Plain-text comment on an exception

Port Forwarding settings

The Port Forwarding settings are used for configuring rules that let an appliance forward web traffic sent from a port on a particular host to another port.

Port Forwarding

Settings for configuring port forwarding rules

Table 13-20 Port Forwarding

Option	Definition
Port forwarding rules	List of port forwarding rules

The following table describes an entry in the list of port forwarding rules.

Table 13-21 Port forwarding rules – list entry

Option	Definition
Source host	IP address of a host that is the source of web traffic in a port forwarding rule
Bind IP	Bind IP address
Target port	Port that web traffic from the source host is forwarded to
Destination host	IP address of the host that is the destination of web traffic sent from the source host
Destination port	Port on the destination host used for listening to web traffic coming in from the source host
Comment	Plain-text comment on a port forwarding rule

Static Routes settings

The Static Routes settings are used for configuring routes that always use the same gateway and interface on this gateway when web traffic is routed from an appliance to a particular host.

Static Routes

Settings for static routes under version 4 or 6 of the Internet Protocol

Table 13-22 Static Routes

Option	Definition
Static routes list	List of static routes for transmitting web traffic under version 4 or 6 of the Internet Protocol

The following table describes an entry in the list of static routes.

Table 13-23 Static routes – list entry

Option	Definition
Destination	IP address and (optionally) netmask of the host that is the destination of a static route
Gateway	IP address of the gateway for routing web traffic from the appliance to a host
Device	Interface used on a gateway for a static route
Description	Plain-text description of a static route
Comment	Plain-text comment on a static route

System files

System files contain settings for functions of the appliance system. You can edit these settings using the File Editor.

The settings that are stored in system files include settings of parameters the appliance system uses for network communication, for example, IP addresses, the maximum message size, or the maximum number of messages in a queue.

Other settings are used to configure functions of the appliance system such as logging, access restrictions, and others.

An example for a system file is the */etc/hosts* file, which contains entries for IP addresses and host names, including the local IP address and host name of the appliance itself.

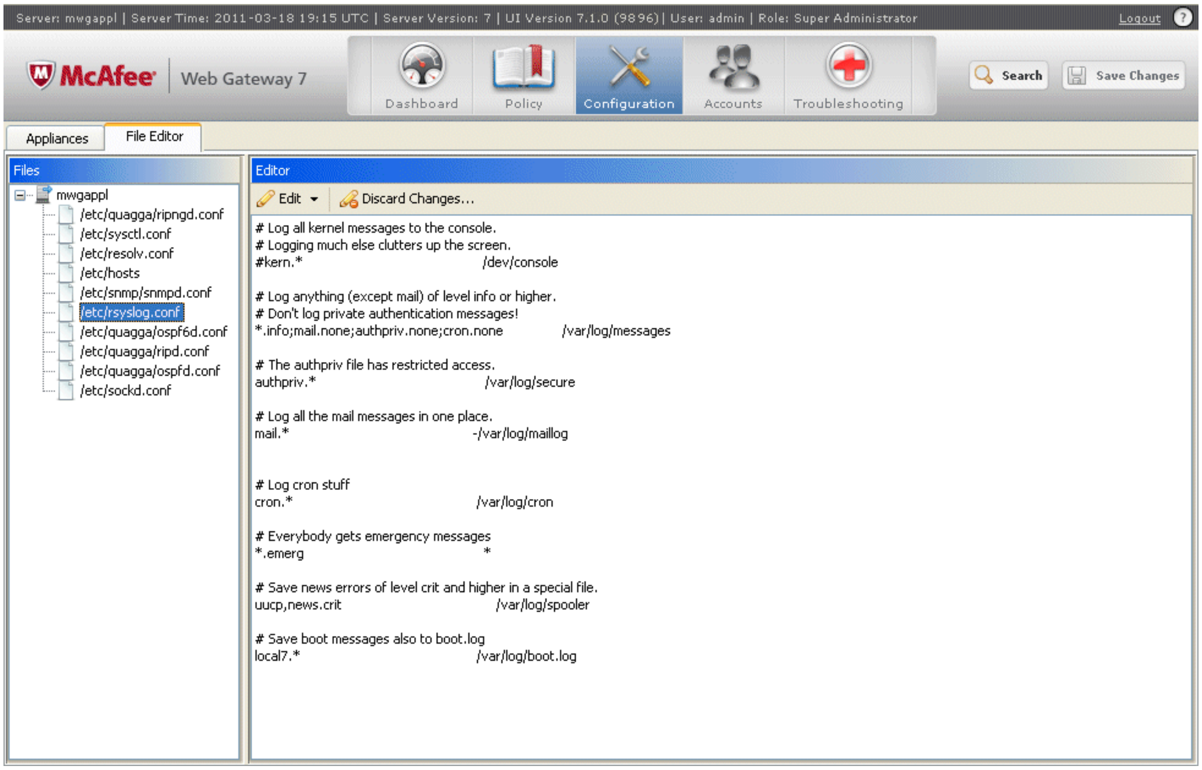
The File Editor allows you to edit the settings in these files. It is accessible on a tab of the user interface.

See also

File Editor tab on page 283

File Editor tab

The **File Editor** tab allows you to edit system files on an appliance.



```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                    /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none              /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                 /var/log/secure

# Log all the mail messages in one place.
mail.*                                    -/var/log/maillog


# Log cron stuff
cron.*                                     /var/log/cron

# Everybody gets emergency messages
*.emerg                                    *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                             /var/log/spooler

# Save boot messages also to boot.log
local7.*                                   /var/log/boot.log
```

Main elements of the File Editor tab

The following table describes the main elements of the **File Editor** tab.

Table 13-24 Main elements of the File Editor tab

Element	Description
Files	Tree structure of appliances with the system files for each appliance
Editor (appears when a system file is selected under **Files**)	Toolbar with items for editing a system file and content pane for displaying the file entries

Editor toolbar

The Editor toolbar provides the following options.

Table 13-25 File Editor toolbar

Option	Definition
Edit	Opens a menu with options for editing the text in system file entries. • **Cut** — Cuts out selected text • **Copy** — Copies selected text • **Paste** — Pastes copied or cut-out text • **Delete** — Deletes selected text • **Select All** — Selects the complete text
Discard changes	Discards text changes. A window opens to let you confirm the discarding.

Database updates

Information retrieved from external databases for use in the filtering process must be updated from time to time.

Web objects are filtered on an appliance in a rule-based process. The filtering rules need information on these objects to know whether they should trigger actions, such as blocking access to an object or allowing it. They rely for this information on special modules (also known as *engines*).

For example, a virus and malware filtering rule relies on the Anti-Malware module (engine) to find out whether an object is virus-infected, or a URL filtering rule relies on the URL Filter module (engine) for URL category information.

The modules retrieve this information, for example, virus signatures stored in DAT files, from external databases. The database updates on an appliance apply to this information.

You can update database information on an appliance using different methods.

- **Manual engine update** — You can manually update database information for the modules of the appliance you are currently logged on to.
- **Automatic engine update** — You can also configure automatic updates in regular intervals for the modules of the appliance you are currently logged on to.

  These updates can retrieve information:

  - **From the internet** — Information is then downloaded from the relevant external databases.

    Database information is for the first time updated in this way immediately after the initial setup of an appliance.

  - **From other nodes in a Central Management configuration** — Information is then downloaded from these nodes. For every node, you can in turn configure whether uploading information from it to other nodes is allowed.

    You can configure these updates when you set up a Central Management configuration, specifying for each node how it should behave with regard to automatic updates.

Update database information manually

You can update database information for the modules of an appliance manually.

The update applies to the modules of the appliance you are logged on to and to those of other appliances that you have included as nodes in a Central Management configuration.

Task

1. Select **Configuration | Appliances**.
2. On the appliances toolbar, click **Manual Engine Update**.

   The update is performed.

Schedule automatic engine updates

You can schedule automatic updates of database information for the modules of an appliance.

When you are running multiple appliances as nodes in a Central Management configuration, you can schedule updates for the modules (also known as *engines*) on the nodes as part of configuring settings for this configuration.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to schedule automatic updates on and click **Central Management Configuration**.
3. Scroll down to **Automatic Engine Updates** and configure update settings as needed.
4. Click **Save Changes**.

14 Central Management

Central Management allows you to administer multiple appliances that you have set up within your network as nodes in a common configuration.

When administering a Central Management configuration, you are dealing mainly with:

- **Nodes** — An appliance can be set up as a node that is onnected to other nodes and can send and receive data to and from them to perform updates, backups, downloads and other activities.
- **Node groups** — Nodes are assigned to different types of node groups that allow data transfer in different ways.
- **Scheduled jobs** — Data can be transferred according to different kinds of schedules that you can configure.

Update schedules can also be configured for the nodes in a Central Management configuration specifying the time when updates should be performed and when not.

Contents

Central Management configuration

In a Central Management configuration, multiple appliances run as nodes and can be administered from any node according to what you have configured.

The nodes in a Central Management configuration are connected within your network as follows:

- Each node is connected to client systems of your network that direct their web traffic to it.
- Nodes are assigned to node groups.
  - Node groups allow common administration activities for the group members, for example, transferring data for updates from one node to another node or several other nodes.
  - There are different types of node groups that allow different kinds of data transfer between the group members.

A Central Management configuration of multiple McAfee Web Gateway appliances is sometimes referred to as a *cluster*. However, it is not a cluster in the sense of a High-Availability cluster with fail-over functions.

The following diagram shows several appliances that run as nodes in a Central Management configuration.

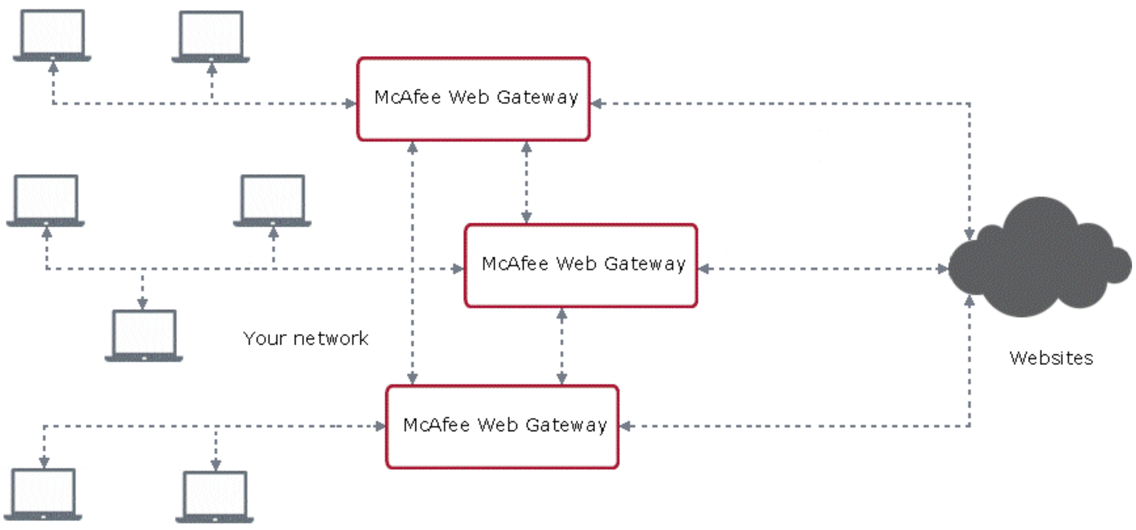


Figure 14-1 Central Management configuration

Types of node groups

The nodes of a Central Management configuration can be assigned to node groups.

Node groups have names and differ with regard to their types. There are the following types of node groups:

- **Runtime group** — A node that is a member of a runtime group can share runtime data with all other nodes in the group.

  Runtime data is data that is created at runtime on an appliance. For example, the amount of time that is left for a user at a given point in time when a quota restriction has been imposed on web usage is runtime data.

  A node can only be a member of one particular runtime group.

- **Update group** — A node that is a member of an update group can share updates with all other nodes in the group.

  A node can only be a member of one particular update group.

- **Network group** — A node that is a member of a network group can immediately connect to all other node in the group.

  A node can be a member of different network groups at the same time.

  When a node is a member of different node groups, for example, of groups A and B, it is possible to transfer data through that node from other nodes in group A that are not members of group B to nodes in group B that are not members of group A.

Scheduled jobs

You can schedule jobs on an appliance, such as creating a configuration backup or downloading files, for execution on a particular time and date or in regular intervals.

You can also configure the schedule on the user interface of the appliance you are currently working on and have the job executed on another node of the same Central Management configuration.

Configure Central Management

You can configure Central Management for multiple appliances within your network to administer them as nodes in a common configuration.

Complete the following high-level steps.

Task

1. Begin with configuring Central Management on the user interface of an appliance within your network and add at least one other appliance as a node in a common configuration.

   Appliances are not by default included as nodes in any Central Management configuration, so all relevant activities must be performed by the administrator.

   For all these activities, you work with the options on the **Appliances** tab of the **Configuration** top-level menu.

   To add a node to a configuration, you need to configure at least the following:

   - Host name or IP address of the appliance you want to add as a node
   - Membership of the node in a network node group

   You can also configure the following settings for a node:

   - IP addresses and ports that should be used for communication with other nodes
   - Membership in runtime and update node groups
   - Scheduled jobs
   - Updates

   Repeat these activities for any other appliance you want to add as a node to the configuration.

2. After initially setting up a Central Management configuration, perform more configuration activities as needed.

   You can, for example, do the following:

   - Review the settings for Central Management on any node of the configuration and modify them

     You can review and modify settings for any node on the user interface of any other node of the configuration.

   - Add one or more new nodes to the configuration

3. Save your changes.

Add an appliance to a Central Management configuration

You can add an appliance as a node to a Central Management configuration and assign it to a network group.

Task

1. On the user interface of an appliance, select **Configuration** | **Appliances**.
2. On the appliances toolbar, click **Add**.

   The **Add Appliance** window opens.
3. In the **Host name or IP** field, type the host name or the IP address of another appliance within your network.
4. From the **Network group** list, select a network group for the appliance.
5. Click **OK**.

   The window closes and the appliance appears on the appliances tree.

   It is a now a node in a Central Management configuration with the appliance you have been working on to complete the addition.

Assign a node to node groups

You can assign an appliance that is a node in a Central Management configuration to node groups of a different types to allow different kinds of data transfer between nodes.

The procedure for assigning a node to a runtime or an update group is nearly the same.

The procedure for a network group is different because a node can be a member in more than one network group.

Tasks

- *Assign a node to a runtime group* on page 290
  You can assign a node to a runtime group by typing the group name in the appropriate input field.
- *Assign a node to an update group* on page 291
  You can assign a node to an update group by typing the group name in the appropriate input field.
- *Assign a node to network groups* on page 291
  You can assign a node to one or more network groups by entering the group name or names into the appropriate list.

Assign a node to a runtime group

You can assign a node to a runtime group by typing the group name in the appropriate input field.

Task

1. On the user interface of an appliance, select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to assign as a node to a runtime group and click **Central Management**.

3 In the **Group runtime** field of the section **This Node Is a Member of the Following Groups**, type the name of the runtime group you want to assign the node to.

When typing the name, be sure to overwrite `all`, which appears in the field as the default name for a runtime group.

This default name is provided to give you the option of not using different runtime groups, but having only one runtime group for *all* nodes.

> If you delete the default `all` and do not enter a name, you assign the node to a group anyway, one that has an empty string as its name.

4 To include another node in the same runtime group, select this node on the appliances tree, click **Central Management** again, and type the same name in the **Group runtime** field.

Repeat this procedure for every node you want to include in the same runtime group.

5 Click **Save Changes**.

Assign a node to an update group

You can assign a node to an update group by typing the group name in the appropriate input field.

Task

1 On the user interface of an appliance, select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to assign as a node to an update group and click **Central Management**.

3 In the the **Group update** field of the section **This Node Is a Member of the Following Groups** type the name of the update group you want to assign the node to.

The procedure is the same as the one for assigning a node to a runtime group.

Also to include other nodes in the group, proceed in the same way as for a runtime group.

4 Click **Save Changes**.

See also
Assign a node to a runtime group on page 290

Assign a node to network groups

You can assign a node to one or more network groups by entering the group name or names into the appropriate list.

Task

1 On the user interface of an appliance, select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to assign as a node to one or more network groups and click **Central Management**.

3 To assign the node to a network group other than the default `all` group, click the **Add** icon on the toolbar of the **Group network** inline list.

The default group is provided to give you the option of not using different network groups, but having only one network group for *all* nodes.

If you want to have more than one network group, you should delete the `all` group or rename it.

The **Add String** window opens.

4 Configure a new network group.

a In the **Name** field, type a name for the network group.

b [Optional] In the **Comment** field, type a plain-text comment on the network group.

c Click **OK**.

The window closes and the new network group appears in the **Group network** inline list.

The node is now a member of this network group.

You can also add multiple network groups at once by clicking the **Add multiple** icon and working with the **Add Strings** window that opens.

In the window, you can enter multiple group names, using a new line for each of them.

The window provides also options for adding the same comment to all groups or add different comments to individual groups.

5 To include another node in the same network group or groups, select this node on the appliances tree, click **Central Management** again, and enter the same group name or names in the **Group network** inline list.

Repeat this procedure for every node you want to include in the same network group or groups.

6 Click **Save Changes**.

Configure the Central Management settings

You can configure the Central Management settings to enable the administration of multiple appliances as nodes in a common configuration.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to configure settings for and click **Central Management**.

The Central Management settings appear on the settings pane.

3 Configure these settings as needed.

4 Click **Save Changes**.

See also

Central Management settings on page 294

Add a scheduled job

You can add a scheduled job to a list of jobs to let them be executed according to a time schedule that you configure.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to add a scheduled job on and click **Central Management**.
3. On the settings pane, expand the **Advanced Scheduled Jobs** section.

   The list of scheduled jobs list appears.
4. On the toolbar above the list, click **Add**.

   The **Add Scheduled Job** window opens.
5. Configure settings for the scheduled job.
6. Click **OK**.

   The window closes and the new scheduled job appears on the job list.
7. Click **Save Changes**.

See also
Central Management settings on page 294

Update the appliance software in a Central Management configuration

To update the appliance software on the nodes of a Central Management configuration, you can perform the update procedure from the user interface of one of the nodes, which is itself the last to be updated.

> **Before you begin**
> Make sure you have created a backup of the current configuration.

Task

1. Install a repository with the product version you want to update to on each appliance that is a node in the configuration.
   a. Log on to an appliance from a system console using SSH.
   b. Run the following command:

      ```
      yum install yumconf-<version number>-mwg
      ```

      `yumconf-<version number>-mwg` is the repository name. The version number is specified using dots, for example, `7.2.0`.
2. Log on to the user interface of one appliance in the configuration.

3 Select **Configuration | Appliances**.

On the appliances tree, select an appliance other than the one you have logged on to.

4 On the toolbar above the settings pane, click **Update appliance software**.

The software on that appliance is updated to the product version that was in the repository.

5 Repeat step 4 for all other appliances on the appliances tree, but leave out the appliance you are working from.

6 When all other appliances that are nodes in the configuration are running their updates, perform the update for the appliance you are working from.

a Select the appliance on the appliances tree.

b Click **Update appliance software**.

> If the nodes in a configuration are assigned to different network groups, with some nodes being members of more than one group, we recommend that you:
>
> - Perform the update procedure from one of the nodes with multiple membership.
> - Update any other node with multiple membership at the end of the procedure.
> - Update the node you are working from last.
>
> For example, you have network group A with nodes 1, 2, 3, 4 and network group B with nodes 3, 4, 5, 6. Then choose node 3 or 4 to perform the update procedure from. Update nodes 1, 2, 5, 6 first, then 4 (if you have chosen 3 to perform the procedure from), and finally 3.

The Central Management configuration is now updated completely.

Central Management settings

The Central Management settings are used for configuring appliances that you administer as nodes in a common configuration.

Central Management Settings

Settings for basic communication parameters of a node in a Central Management configuration

Table 14-1 Central Management Settings

Option	Definition
IP addresses and ports of this node for Central Management communication	List of IP addresses and port numbers that a node uses to communicate with other nodes in a Central Management configuration
Timeout for distributing messages to other nodes	Time (in seconds) that is allowed for another node to respond to a message from the current node The time can range from 10 to 600 seconds. It is set on a slider scale.

The following table describes the elements of an entry in the IP addresses and ports list.

Table 14-2 IP addresses and ports – List entry

Option	Definition
String	IP address and port number for a node
Comment	Plain-text comment on an IP address and a port number

Advanced Management Settings

Settings for advanced administration of a Central Management configuration

Table 14-3 Advanced Management Settings

Option	Definition
Multiplier for timeout when distributing over multiple nodes	Factor for increasing the time interval that has been configured under *Timeout for distributing messages to other nodes* in the *Central Management Settings* section. Increasing the time interval gives messages more time to proceed from one node to another, from there to the next node, and so on. The interval can be increased by a value between 1 and 2. The value is set on a slider scale.
Node priority	Priority that a node takes within a node group The highest priority is 1. If the configuration data on a node is no longer synchronized with that of other nodes, for example, because the node has been down for some time, the node receives the most recent configuration data from the node with the highest priority. If this is not your intention, make sure that all nodes have the same priority, which is also the recommended setting. The priority of a node can range from 1 to 100. It is set on a slider scale.
Allow a GUI server to attach to this node	When selected, a server providing an additional user interface for the appliance is allowed to connect to the node.
Allow to attach a GUI server from non-local host	When selected, a server with an additional user interface that is not running on the current node is allowed to connect to the node.
GUI control address	IP address and port number the additional user interface uses for connecting to the current node
GUI request address	IP address and port number of this server used when sending requests to it
Contact other nodes unencrypted	When selected, messages sent from this node to other nodes in the configuration are not encrypted. However, authentication using certificates is still performed.
Enable IP checking for other nodes	When selected, the IP address can be verified when messages are sent from this node to other nodes in the configuration. This function is intended to increase web security, but can lead to problems for some network setups, for example, NAT setups.

Table 14-3 Advanced Management Settings *(continued)*

Option	Definition
Allowed time difference	Time difference (in seconds) allowed for accepting configuration changes The number of seconds can range from 10 to 600. It is set on a slider scale.
Enable version checking for other nodes	When selected, the version of the appliance software is checked before configuration changes are distributed between nodes. Configuration changes are not distributed to a node if the version of the appliance software on this node does not match the version on the node that distributes the changes. • **Level of version check** – Level of thoroughness when verifying the version of the appliance software The verification level can range from 1 (very relaxed: only the major version number must match) to 6 (very strict: also the build number must match) It is set on a slider scale.

This Node is a Member of the Following Groups

Settings for including a node in a group of nodes

Table 14-4 This Node is a Member of the Following Groups

Option	Definition
Group runtime	Group of a node, in which runtime data can be shared with all nodes in the group, for example, time quotas
Group update	Group of a node, in which updates can be shared with all nodes in the group
Group network	Group of a node, in which the node can immediately connect to all other nodes in the group A node can be a member of more than one network group. In this case, the nodes of a group that a node is a member of can connect through this node to nodes of another group that this node is also a member of. All groups that a node is a member of are listed in the Group network list.

The following table describes the elements of a list entry in the group network list.

Table 14-5 Group network – List entry

Option	Definition
String	Name of a network node group
Comment	Plain-text comment on a network node group

Automatic Engine Updates

Settings for scheduling automatic updates of database information for modules used in the filtering process

Table 14-6 Automatic Engine Updates

Option	Definition
Enable automatic updates	When selected, database information is automatically updated.
Allow to download updates from the internet	When selected, database updates are downloaded from the internet.

Table 14-6 Automatic Engine Updates *(continued)*

Option	Definition
Allow to download updates from other nodes	When selected, database updates are downloaded from other nodes in a Central Management configuration.
Update interval	Time (in minutes) to elapse before database information is again updated The time is set on a slider scale. Allowed values range from 15 to 360.
CRL update interval	Time (in hours) to elapse before certificate revocation lists used in filtering SSL-secured web traffic are updated This update uses a method that differs from those of other updates and must therefore be configured separately. The time is set on a slider scale Allowed values range from 3 to 168.
Enable update proxies	When selected, proxy servers are used for routing updated database information.
Update proxies (fail over)	List of proxy servers used for routing updated database information The proxy servers are used in failover mode. The first server on the list is tried first and only if the configured timeout has elapsed is the next server tried.

The following table describes the elements of an entry in the Update proxies list.

Table 14-7 Update proxies – List entry

Option	Definition
Host	Host name or IP address of a server that is used as a proxy for routing updates
Port	Port on a proxy that listens for update requests
User	User name of a user who is authorized to access a proxy for routing updates
Password	Password for this user
Comment	Plain-text comment on a proxy

Advanced Update Settings

Settings for advanced update functions

Table 14-8 Advanced Update Settings

Option	Definition
Allow to upload updates to other nodes	When selected, updated database information can be uploaded from the appliance (as a a node in a Central Management configuration) to other nodes.
The first time an update starts, it should wait an appropriate time before starting	Time (in seconds) to elapse before an update is started Allowed values range from 5 to 1200

Table 14-8 Advanced Update Settings *(continued)*

Option	Definition
The first time an automatic update starts, it uses the startup interval to update	Time (in seconds) to elapse between attempts to start an automatic update for the first time During an update, the coordinator subsystem, which stores updated information on the appliance, tries to connect to the appliance core, where the modules reside that use this information. A low value for this interval can therefore speed up updates because it reduces the time the coordinator might have to wait until the core is ready to receive data. Allowed values range from 5 to 600
Try to update with start interval	Maximum number of attempts (1 to 9) the appliance makes when trying to start an update
Use alternative URL	URL of an update server that is used instead of the default server
Verify SSL tunnel	When selected, a certificate sent to a node by an update server in SSL-secured communication is verified.
No updates should be made in defined time window	List of entries for daíly time slots during which no updates of database information should be made

The following table describes the elements of an entry in the time slot list.

Table 14-9 Time slot – List entry

Option	Definition
Start of time slot (hour)	Hour when a daily time slot begins
Start of time slot (minute)	Minute in the hour when a daily time slot begins
Start of time slot (second)	Second in the minute when a daily time slot begins
End of time slot (hour)	Hour when a daily time slot ends
End of time slot (minute)	Minute in the hour when a daily time slot ends
End of time slot (second)	Second in the minute when a daily time slot ends
Comment	Plain-text comment on a time slot

Advanced Subscribed Lists Settings

Settings for advanced subscribed lists functions

Table 14-10 Advanced Subscribed Lists Settings

Option	Definition
Allow to download customer subscribed lists	When selected, customer subscribed lists can be downloaded from the current appliance. if the appliance is a node in a Central Management configuration and this option is also selected on other nodes, one of the nodes will download the lists. If you want a particular node to download the lists, you need to make sure the option is deselected on every other node. When a node is restarted and one or more subscribed lists are configured on this node, list content is downloaded to ensure a valid configuration. ℹ The download is performed regardless of whether this download option is selected or not. When a node is added to a configuration with other nodes that have subscribed lists configured, list content is downloaded for these lists onto the new node. To reduce internal traffic, the download is performed without prior communication with other nodes. ℹ The download is performed regardless of whether this download option is selected or not.

Manual Engine Updates

Setting for performing manual updates of database information for modules used in the filtering process

Table 14-11 Manual Engine Updates

Option	Definition
Manual Engine Update	Updates database information for modules used in the filtering process immediately Database information is only updated for the modules on the appliance you are currently working on

Handle Stored Configuration Files

Settings for storing configuration file folders on disk

Table 14-12 Handle Stored Configuration Files

Option	Definition
Keep saved configuration folders for a minimal time	Time (in days) that configuration file folders are at least stored on disk The number of days can range from 1 to 100.
Keep minimal number of configuration folders	Number of configuration file folders that are at least stored on disk at any time The number can range from 1 to 100.
Keep minimal number of packed folders	Number of packed configuration file folders that are at least stored on disk at any time Configuration folders are packed when the minimal time configured for storing them on disk has elapsed and the minimal number of folders stored on disk at any time would be exceeded if they were stored unpacked any longer. The number of folders can range from 1 to 100.

Advanced Scheduled Jobs

Settings for scheduled jobs

Table 14-13 Advanced Scheduled Jobs

Option	Definition
Job list	List of scheduled jobs

The following table describes the elements of a list entry.

Table 14-14 Job list entry

Option	Definition
Start job	Time setting for starting a scheduled job, for example, *hourly*, *daily*, *once*
Start job immediately if it was not started at its original schedule	Information on whether a scheduled job is started immediately if this has not happened according to the originally configured schedule
Job	Type of job, for example, *Backup Configuration*
Unique job ID	ID of a scheduled job
When this job has finished run job with ID	ID of a job that is run immediately after this job
Comment	Plain-text comment on a scheduled job

Add Scheduled Job window

Settings in the window for adding a scheduled job

- **Time Settings** – Settings for the time when a scheduled job is started
- **Job Settings** – Settings for the type and ID of a scheduled job
- **Parameter Settings** – Settings for additional parameters of a scheduled job

  These settings differ for each job type as follows:

  - (Backup configuration settings) – Settings for a scheduled job that creates a backup of an appliance configuration
  - (Restore backup settings) – Settings for a scheduled job that restores a backup of an appliance configuration
  - (Upload file settings) – Settings for a scheduled job that uploads a file to an external server using the HTTP or HTTPS protocol
  - (Download file settings) – Settings for a scheduled job that downloads a file to the appliance using the HTTP or HTTPS protocol

  For a scheduled job that performs a yum update, there are no additional parameter settings.

Table 14-15 Time Settings

Option	Definition
Start job	List for selecting a time setting • **Hourly** – Starts a scheduled job every hour • **Daily** – Starts a scheduled job once on a day • **Weekly** – Starts a scheduled job once in a week • **Monthly** – Starts a scheduled job once in a month • **Once** – Starts a scheduled job only once • **Activated by other job** – Starts a scheduled job after another job has been completed
(Time parameter settings)	Settings specifying the parameters for a time setting, for example, the minute in an hour when a job scheduled for hourly execution should be started Which time parameter settings are shown depends on the selected time setting. For example, if you have selected *Hourly*, you can configure the minute in an hour, but not the day in a month. • **Minute** – Minute in an hour • **Hour** – Hour on a day • **Day of month** – Day in a month • **Enter day of week** – List for selecting a day in the week • **Month** – Month in a year (specified by a number from 1 to 12) • **Year** – Year (four digits)
Start job immediately if it was not started at its original schedule	When selected, a scheduled job is started immediately if this has not happened according to the originally configured schedule. This can be the case, for example, when an appliance is temporarily shut down due to overload and a job was scheduled to run during this downtime. The job is then executed as soon as the appliance is up again.

Table 14-16 Job Settings

Option	Definition
Job	List for selecting the type of a scheduled job • **Backup configuration** – Creates a backup of an appliance configuration • **Restore backup** – Restores a backup of an appliance configuration • **Upload file** – Uploads a file to an external server using the HTTP or HTTPS protocol • **Download file** – Downloads a file onto the appliance using the HTTP or HTTPS protocol • **Yum update** – Performs a yum update on an appliance configuration ⓘ This scheduled job type is not available when an appliance runs in a FIPS-compliant mode.
Unique job ID	String that uniquely identifies a scheduled job The characters specified in this string are case-sensitive.
Job description	Optional description of a scheduled job in plain-text format

Table 14-16 Job Settings *(continued)*

Option	Definition
When this job has finished run job with ID	ID of a scheduled job that is to run immediately after the job configured here has finished For this job, you must have configured the *Activated by other job* time setting.
Execute job on remote node	List for selecting other nodes of the configuration to execute a scheduled job The list displays the host names for the other nodes. The scheduled job that you configure on this appliance is executed with its time and parameter settings on the selected node or nodes. A message is sent to the other node or nodes to inform them about the scheduled job.

Table 14-17 Parameter Settings – Backup configuration

Option	Definition
Use most recent configuration	When selected, the scheduled job creates a backup from the most recent appliance configuration Format: |*<path name>/<file name with extension>*
Backup configuration path	Name of the path to the folder where the configuration is stored that should be used for the backup Format: */opt/mwg/storage/default/configfolder* This setting is only available when **Use most recent configuration** is deselected.
Save configuration to path	Path and file name for a backup configuration Format: */<path name>/<file name with file name extension>* You must set user rights for the folder you want to store the backup configuration in, making the appliance the owner who is allowed to write data into the folder. On the command line provided, for example, by a serial console, run the appropriate commands to create a folder or change the rights for an existing folder.

Table 14-18 Parameter Settings – Restore backup

Option	Definition
Restore backup from file	Path and file name for a file that should be used to restore a backup Format: |*<path name>/<file name with extension>*
Only restore policy	When selected, a scheduled job backs up only settings related to the web security policy that was implemented on an appliance. Other settings, for example, settings needed for connecting an appliance to a network are not restored.
Lock storage during restore	When selected, no other files can be stored on the appliance until the scheduled job has completely restored the backup configuration.
Password	Password submitted for basic authentication
Set	Opens the **New Password** window for setting a password When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password. This setting is only available when **Enable basic authentication** is selected.

Table 14-19 Parameter Settings – Upload file

Option	**Definition**
File to upload	Path and file name for a file that should be uploaded Format: |*<path name>/<file name with extension>*
Destination to upload file to	Name of the path to a server that a file should be uploaded to under the HTTP or HTTPS protocol and file name for storing the file on the server Format: *http|https: //<URL>/<file name with extension>*
Enable basic authentication	When selected, basic authentication is required for uploading a file.
User name	User name submitted for basic authentication This setting is only available when **Enable basic authentication** is selected.
Password	Password submitted for basic authentication
Set	Opens the **New Password** window for setting a password When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password. This setting is only available when **Enable basic authentication** is selected.

Table 14-20 Parameter Settings – Download file

Option	**Definition**
URL to download	URL for the location of a file that should be downloaded under the HTTP or HTTPS protocol and name of the file Format: *http|https: //<URL>/<file name with extension>*
Save downloaded file to	Path to the location where a downloaded file should be stored and file name for storing the file Format: |*<path name>/<file name with extension>*
Enable basic authentication	When selected, basic authentication is required for downloading a file
User name	User name submitted for basic authentication This setting is only available when *Enable basic authentication* is selected.
Password	Password submitted for basic authentication
Set	Opens the **New Password** window for setting a password When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password. This setting is only available when *Enable basic authentication* is selected.

15 Web Hybrid

Settings for filtering web objects can be synchronized between McAfee Web Gateway and McAfee SaaS Web Protection Service, which is a McAfee product for "in the cloud" web security. Both products work together in what is known as the Web Hybrid Security solution.

Contents

Synchronizing settings for the Web Hybrid Security solution

When McAfee Web Gateway and McAfee SaaS Web Protection Service work together in the Web Hybrid Security solution, web filtering settings need to be synchronized between the products to allow for a common web security policy.

The McAfee Web Hybrid Security solution enables you to enforce a common web security policy for users who are working on systems within your corporate network, as well as for those who are working on their systems from home or when traveling.

For this purpose, the solution uses a combination of on-premise products, such as McAfee Web Gateway and cloud-based products, such as McAfee SaaS Web Protection Service.

The synchronization of web filtering settings between the two products works both ways. When you apply changes to the web filtering settings on McAfee Web Gateway, these changes are also applied on McAfee SaaS Web Protection Service.

In the same way, changes that the administrator for McAfee SaaS Web Protection Service applies on that product are also applied on McAfee Web Gateway.

An internal interface known as REST (Representational State Transfer) interface handles the data transfer.

To let the synchronization become effective, you need to configure several settings on the side of McAfee Web Gateway, for example, the host name or IP address of the portal that provides access to McAfee SaaS Web Protection Service.

If you are administering multiple McAfee Web Gateway appliances as nodes in a Central Management configuration, you can perform the synchronization on any node of the configuration.

For more information on the Web Hybrid Security solution, see the *McAfee Web Hybrid Security Solution Deployment Guide*.

Web filtering settings for synchronization

Different types of web filtering settings can be synchronized between McAfee Web Gateway and McAfee SaaS Web Protection Service.

Web filtering settings for synchronization between the two products include:

- **Policy settings** — Settings that specify parameters of web security policies, such as host names or URL categories
- **User group settings** — Settings that specify user groups

Different ways of handling these settings are possible on a McAfee Web Gateway appliance.

Policy settings for synchronization

Particular web filtering settings are combined on McAfee SaaS Web Protection Service to create a web security policy. These are settings for the following parameters:

- Name of a policy
- Description of a policy
- Enable/disable Anti-Malware filtering
- Enable/disable SafeSearch filtering
- Allowed URL categories
- Blocked URL categories
- Trusted web sites by host names
- Blocked web sites by host names
- Trusted web sites by IP addresses
- Blocked web sites by IP addresses

Settings for these parameters can be changed on both McAfee Web Gateway and McAfee SaaS Web Protection Service and the changes are synchronized betweeen the two products.

User group settings for synchronization

User group settings include the groups of users that are particular web security policies are assigned on McAfee SaaS Web Protection Service.

These settings can be changed on McAfee SaaS Web Protection Service. Users can be added to a group and new groups can be created. On McAfee Web Gateway, these settings can only be viewed, not changed.

However, any change on McAfee SaaS Web Protection Service is synchronized, so the current settings can alway be viewed on McAfee Web Gateway.

Configure synchronization settings

To enable the synchronization of web filtering settings between McAfee Web Gateway appliance and the McAfee SaaS Web Protection Service, you need to configure appropriate settings.

Task

1. Select **Configuration** | **Appliances**.
2. Select the appliance you want to configure synchronization settings for and click **Web Hybrid**.

   The settings for synchronization between McAfee Web Gateway and McAfee SaaS Web Protection Service appear on the settings pane.

3 Configure these settings as needed.

4 Click **Save Changes**.

See also
Web Hybrid settings on page 307

Web Hybrid settings

The Web Hybrid settings are used for configuring the synchronization of web filtering settings between McAfee Web Gateway and McAfee SaaS Web Protection Service.

Web Hybrid Configuration

Settings for synchronizing web filtering settings

Table 15-1 Web Hybrid Configuration

Option	Definition
SaaS address	IP address or host name of the portal that provides access to the McAfee SaaS Web Protection Service
SaaS customer ID	Identifies a customer who runs the McAfee SaaS Web Protection Service.
SaaS administrator account name	User name of the account for the administrator who manages McAfee SaaS Web Protection Service The name that you specify here must be the name of a user of McAfee SaaS Web Protection Service who has been assigned the role of *Customer Admin*.
SaaS administrator account password	Password for the administrator account This must be the password for the user of McAfee SaaS Web Protection Service that is mentioned under **SaaS administrator account name**. Click **Set** to open a window for setting a new password.
Enable synchronization to SaaS	When selected, changes in the web filtering settings on McAfee Web Gateway are applied to the corresponding settings on McAfee SaaS Web Protection Service.
Enable synchronization from SaaS	When selected, changes in the web filtering settings on McAfee SaaS Web Protection Service are applied to the corresponding settings on McAfee Web Gateway.
Local policy changes will be uploaded immediately to SaaS	When selected, changes in the policy settings that you apply on McAfee Web Gateway are immediately uploaded to McAfee SaaS Web Protection Service.
Local policy changes will be uploaded within the same interval as defined below	When selected, changes in the policy settings that you apply on McAfee Web Gateway are uploaded to McAfee SaaS Web Protection Service after the time interval configured below has elapsed. Allowed values for the time interval range between 10 and 60 minutes. The time interval is set on a slider scale.

Web Hybrid Actions

Options for performing the synchronization of web filtering settings

Table 15-2 Web Hybrid Configuration

Option	Definition
Synchronize to SaaS	Performs the immediate synchronization of web filtering setttings on McAfee Web Gateway with the corresponding settings on McAfee SaaS Web Protection Service.
Synchronize from SaaS	Performs the immediate synchronization of web filtering setttings on McAfee SaaS Web Protection Service with the corresponding settings on McAfee Web Gateway

16 REST interface

An interface is provided that allows you to administer an appliance without being logged on to its standard user interface. This alternative interface is known as the REST (Representational State Transfer) interface.

Using the REST interface, you can perform different kinds of activities on a particular appliance or on others that are connected to it.

- **Actions** — Shutdown an appliance, restart it, flush the cache, create a configuration backup, and perform several other activities
- **File handling** — Access system, log, and troubleshooting files to perform activities such as downloading, modifying, deleting, and others
- **List handling** — Work with lists and list entries to perform activities such as adding, modifying, deleting, and others

The usual way to perform these activities is to let them be executed by a suitable script.

Contents

Prepare use of the REST interface

To let users work with the REST interface, you need to enable it on the standard user interface of an appliance and permit access to it.

Tasks

- *Enable use of the interface* on page 310
  You can enable the use of the REST interface for completing administration activities on an appliance.
- *Give permission to access the interface* on page 310
  You must add permission to access the REST interface to an administrator role for those users who are supposed to work with the interface.

Enable use of the interface

You can enable the use of the REST interface for completing administration activities on an appliance.

Task

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to administer using the REST interface and click **User Interface**.
3. Under **UI Access**, select **Enable REST interface over HTTP** or **Enable REST interface over HTTPS** as needed.
4. Click **Save Changes**.

Give permission to access the interface

You must add permission to access the REST interface to an administrator role for those users who are supposed to work with the interface.

Task

1. Select **Accounts** | **Administrator Accounts**.
2. In the **Roles** area, select an administrator role and click **Edit**.

   The **Edit Role** window opens.
3. Select **REST interface accessible**.
4. Click **OK** to close the window.
5. Click **Save Changes**.

You can now assign this administrator role to the appropriate users.

Instead of adding access permission to an existing role, you can also create a new role with this permission and name it, for example, *REST Admin*.

Working with the REST interface

When working with the REST interface, you use it for sending HTTP or HTTPS requests to perform activities on one or several appliances.

You can send individual requests that are immediately processed or use requests in a script, for example, in a bash script. The latter is the typical use.

Requests are sent to the REST interface using a client of an appliance, which provides a server to process the requests and send responses. You are assigned a particular work space on the server, so to apply some types of changes, you need to send a request to commit them to let them become effective.

When logging on to the REST interface on an appliance, you authenticate and are provided with a session ID in return. You can then send HTTP or HTTPs requests to execute actions and work with files and lists on the appliance. You can do the same on other appliances that are connected as nodes in a Central Management configuration to the one you are logged on to.

The REST interface is provided in a particular format known as the ATOM format

As your client for communicating with the interface server, you can use a data transfer tool, for example, *curl* (Client for URLs).

Sample script for sending a request

The following is an example of a bash script that sends a request to the REST interface using curl. The purpose of the request is to create a configuration backup.

The script does basically the following:

- Logs on and authenticates to the REST interface on an appliance
- Sends a request to create a backup file
- Logs off again

The script also uses a variable for the URL that is specified in the request for logging on to the REST interface. The variable is set at the beginning.

```
# !bin/bash

# Set URL variable for access to REST interface

REST="http://localhost:4711/Konfigurator/REST"

## Log on and authenticate

curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login"

## Create backup file

curl -b cookies.txt -X POST "$REST/backup" -o filename.backup

## Log off again

curl -b cookies.txt -X POST "$REST/logout"
```

Using curl as the data transfer tool

To send requests to the REST interface on an appliance, you can use curl as the data transfer tool.

A request sent with curl usually has three main parts: the *curl* command, one or several options, and a URL.

For example, in the following backup request:

```
curl -b cookies.txt -X POST "$REST/backup" -o filename.backup
```

the curl command appears with the *-b* option for sending cookies that have been collected in a text file and the *-o* option, which stores the output of the request in another file. The - *X* option is for the request method.

The URL is specified as a variable that has the IP address, port number, and other information needed for access to the REST interface on an appliance as its value. It is followed by the name of the activity that should be performed.

Using these and other options of curl together with the appropriate URLs, you can send requests to the REST interface on an appliance to perform activities as needed.

The curl data transfer tool is available under Linux and other UNIX operating systems and described in full detail, for example, on the *curl* man page.

Request methods

The request method is specified in curl by the *-X* option. When working with the REST interface on an appliance, the GET, POST, PUT, and DELETE methods can be used, for example, as follows:

`curl -X POST` <URL>

If no request method is specified, GET is used as the default method.

Headers

When a header is sent with a request, it is specified by the *-H* option, for example, as follows:

```
curl -H <header name>:<header value> -X POST <URL>
```

You can send multiple headers within one request, repeating the *-H* option letter before each header.

```
curl -H <header name 1>:<header value 1> -H <header name 2>:<header value 2> <...> -X
POST <URL>
```

A request normally includes an *Accept* header that has *application/atom+xml* as its value. In curl *Accept: */** is sent as a default, which is accepted by the REST interface, so you can leave out this header in many cases.

However, if you send data in the body of a request, you need to include the *Content-Type* header with *application/atom+xml* as its value. Then you also need to include the *Content-Length* header and set it correctly. The latter is done in curl by default, so you need not do it explicitly when using this tool.

If you want to include the header of the response you get upon a request in its output, you need to insert the *-i* option.

```
curl -i -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST
"$REST/login"
```

The *-v* option creates verbose output, which means that also the request header is included.

URLs

A URL in a request specifies a protocol, which can be HTTP or HTTPS in communication with the REST interface, the IP address or host name and the port number of the appliance that a request is sent to, and the internal path on the appliance to the REST interface.

This is followed by the name of the activity that should be performed and further parameters if there are any.

As the REST interface is located within the configurator subsystem of an appliance, the internal name of this subsystem, which is *Konfigurator*, appears in the URL.

A URL in, for example, a logon request, could therefore look as follows:

```
curl -X POST "HTTP://localhost:4711/Konfigurator/REST/login?userName=myusername
&pass=mypassword
```

In this request, the URL has also query parameters for the logon credentials. Query parameters are introduced by a *?* (question mark) and separated by an & (ampersand), as shown. A URL can also have matrix parameters, which are introduced by a *;* (semicolon).

For correct URL encoding, spaces in a URL must be filled with the symbols *%20*. So, for example, *Bob Smith* becomes *Bob%20Smith*.

You can use a variable within a URL for easier code writing and reading. For example, if you have set the *$REST* variable accordingly, the above request could look as follows:

```
curl -X POST "$REST/login?userName=myusername&pass=mypassword
```

Sending data in the request body

For sending data in the body of a request, the *-d* option is used, followed by the name of the file that contains the data.

```
curl -b cookies.txt -X POST -d "file.txt" "$REST/list?name=newlist&type=string"
```

If you are sending only binary data, the option to use is - - *data-binary*.

```
curl -b cookies.txt --data-binary @file.backup -X POST "$REST/restore" -H
"Content-Type: text/plain; charset=UTF-8"
```

You can use the symbol @ after the option name to indicate a file name.

See also
Sample scripts for working with the REST interface on page 325

Authenticating to the interface

Before you can use the REST interface to perform any activities on an appliance you need to authenticate.

To authenticate you submit user name and password in the logon request that you send to the REST interface.

There are the following two ways to submit them:

- Using query parameters
- Using an authentication header

After a successful authentication, the response contains the session ID, which you must include in each of your following requests.

Using query parameters for authentication

You can submit your credentials with query parameters that you add to the URL in your logon request.

```
curl -i -X POST "$REST/login?userName=myusername&pass=mypassword"
```

Using an authentication header

You can also use the Basis Access Authentication method to authenticate, which requires you to submit your credentials in an authentication header.

```
curl -i -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login
```

In the authentication header, the string after *Authorization: Basic* is the Base64-encoded representation of your user name and password.

Session ID

The session ID is sent to you in the reponse to your logon request. The session ID looks, for example, as follows:

```
D0EFF1F50909466159728F28465CF763
```

It is either contained in the response body:

```
<entryxmlns="http://www.w3.org/2005/
Atom"><contenttype="text">D0EFF1F50909466159728F28465CF763</content></entry>
```

or in a Set-Cookie header:

```
Set-Cookie: JSESSIONID=D0EFF1F50909466159728F28465CF763
```

In the requests of the session that follow the logon request, you need to include the session ID as JSESSIONID.

For easier code writing and reading, you can set a variable to the value of the ID and use it for including the ID.

```
export SESSIONID=D0EFF1F50909466159728F28465CF763
```

You can append the ID as a matrix parameter to the URL, preceded by a semicolon.

```
curl -i "$REST/appliances;jsessionid=$SESSIONID"
```

Alternatively, you can send the ID in a Cookie header.

```
curl -i -H "Cookie: JSESSIONID=$SESSIONID" "$REST/appliances"
```

The option *-c* in curl allows you to collect all cookies in a text file, which is then sent with subsequent requests.

```
curl -i -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST
"$REST/login"
```

For sending a cookie file with a request, the option *-b* is used:

```
curl -i -b cookies.txt "$REST/appliances"
```

Requesting resources

A request sent to the REST interface regarding system files, log files, lists, and some other items is considered to be a request for resources.

The response to a request for resources can be one of the following:

- **Entry** — An entry delivers information in xml format about an individual resource, such as its ID, name, or the URL that can be used to access it
- **Feed** — A feed delivers information in xml format about a collection of resources.

  A feed can, for example, be a list of appliances that are available as nodes in a Central Management configuration, or a list of all lists that exist on an appliance, or a list of all lists of a particular type.
- **Binary data** — Binary data is delivered in a file that you requested for downloading.

A response can also be empty. This is the case when the requested data is not available.

Reducing xml data overhead

You can reduce the xml data overhead that you receive with a response, by including an appropriate Accept header in a request for resources. For this purpose, the header value must be *application/mwg+xml*.

Instead of an entry in the normal Atom format, you will then receive only the xml data from the content part of that format.

Instead of a feed in Atom format, you will only receive a list of IDs for the resources you asked for.

Similarly, you can reduce xml data overhead when working with the resources, for example, when modifying them. For this, you need to set the Content-Type header to *application/mwg+xml*.

Paging a feed

When requesting a feed, you can use paging, which means you can ask for a feed that is divided into pages.

Paging information is specified by query parameters that are added to the URL in a request. The following two parameters can be used:

- **PageSize** — Maximum number of elements on a page
- **Page** — Page number

A request for a feed that uses paging could look as follows:

```
curl -i -b cookies.txt "$REST/list?pageSize=10&page=4"
```

If a feed is, for example, a list of 35 lists, the *pageSize* parameterin the above request divides it up into four pages, three of which contain ten lists, while the last one contains only five. The last page is also the one that is delivered.

Navigating within a feed

To allow navigation within a feed, the xml file that you receive contains appropriate links.

Using these links, you can go to the current, next, previous, first, and last page, respectively.

Performing basic activities

When working with the REST interface, you can perform several basic activities within your working environment, such as logging on and off, committing changes, creating a configuration backup, and others.

The POST request method is used for performing all these activities. A particular activity is specified by a parameter that is added to the URL of a request.

For example, the following is a request to log off from the REST interface on an appliance:

```
curl -i -b cookies.txt -X POST "$REST/logout"
```

Parameters for basic activities are as follows:

- **login** — Log on
- **logout** — Log off
- **heartbeat** — Keep a session alive
- **commit** — Commit changes
- **discard** — Discard changes
- **backup** — Back up the configuration
- **restore** — Restore the configuration

In addition to performing these activities, you can request information on the version of REST interface, as well as that of the standard user interface of the appliance you are currently working on.

Logging on

To log on to the REST interface on an appliance, the *login* parameter is used in a request. Within this request you also submit your credentials for authentication, for example, in the following way:

```
curl -i -X POST "$REST/login?userName=myusername&pass=mypassword"
```

If authentication is performed successfully, the response to the logon request provides a session ID.

Logging off

To log off from the REST interface on an appliance, the *logout* parameter is used.

```
curl -i -b cookies.txt -X POST "$REST/logout"
```

Logging off deletes the session information and discards the changes made in a session that would need to be, but have not been committed.

Keeping a session alive

Using the *heartbeat* parameter in a request keeps the session alive that you are currently working in.

```
curl -i -b cookies.txt -X POST "$REST/heartbeat"
```

Committing changes

To commit changes that have been made to items such as system files, log files, lists, and others on an appliance, the *commit* parameter is used.

```
curl -i -b cookies.txt -X POST "$REST/commit"
```

Discarding changes

To discard changes that have been made to items such as system files, log files, lists, and others on an appliance, the *discard* parameter is used.

```
curl -i -b cookies.txt -X POST "$REST/discard"
```

Backing up the configuration

To create a configuration backup for the appliance you are currently working on, the *backiup* parameter is used.

```
curl -b cookies.txt -X POST "$REST/backup -o filename.backup"
```

When backing up or restoring a configuration, no response header is required as part of the output, so the *-i* option needs not to be included in the request.

Restoring the configuration

To restore the configuration of the appliance you are currently working on, the *restore* parameter is used. You also need to specify a Content-Type header for the type of the backup file.

```
curl -b cookies.txt --data-binary @filename.backup -X POST "$REST/restore" -H
"Content-Type: text/plain;charset=UTF-8"
```

Requesting version information

To request information on the version of the REST interface or the standard user interface of the appliance you are currently working on, you can use the *version* parameter.

Using the parameter alone in a request retrieves a feed in xml format with the versions of both interfaces.

```
curl -i -b cookies.txt -X GET "$REST/version"
```

If you are only interested in version information for one of the interfaces, you can send the following request for the REST interface:

```
curl -i -b cookies.txt -X GET "$REST/version/mwg-rest"
```

and this one for the standard user interface:

```
curl -i -b cookies.txt -X GET "$REST/version/mwg-ui"
```

See also
Sample scripts for working with the REST interface on page 325

Working on individual appliances

After logging on to the REST interface on one appliance, you can perform activities on any other appliance that is connected. Individual appliances are identified in requests by their UUIDs.

To find out about the UUID (Universal Unique Identifier) of an individual appliance, you can request a feed of all appliances that are connected as nodes in a Central Management configuration to the one you are currently working on.

The feed includes a list of the UUIDs for all nodes. A UUID looks, for example, as follows:

```
081EEDBC-7978-4611-9B96-CB388EEFC4BC
```

A GET request is sent to retrieve the feed, with the *appliances* parameter appended to the URL.

```
curl -i -b cookies.txt -X GET "$REST/appliances"
```

You can then identify an individual appliance by its UUID and, for example, shutdown this appliance with a POST request, appending the *action* parameter and *shutdown* as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/shutdown"
```

You can repeat this action or any other activity on all individual appliances that the feed delivered UUIDs for, for example, by running an appropriate script.

Actions

When working with the REST interface, actions are those activities that are preceded by the *action* parameter in a request. They do not involve a modification of resources and are performed instantly, which means no request to commit them is required.

Action names are as follows:

- **restart** — Restart an appliance
- **shutdown** — Shut down an appliance
- **flushcache** — Flush the cache
- **rotateLogs** — Rotate log files
- **rotateAndPushLogs** — Rotate and push log files
- **license** — Import a license

Restarting an appliance

To restart an appliance, *restart* is used as the action name in a request.

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/action/restart"
```

Shutting down an appliance

To shut down an appliance, *shutdown* is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/shutdown"
```

Flushing the cache

To flush the cache on an appliance, *flushcache* is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/flushcache"
```

Rotating log files

To rotate log files on an appliance, *rotateLogs* is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/rotateLogs"
```

Rotating and pushing log files

To rotate and push log files on an appliance, *rotateAndPushLogs* is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/" <UUID>/action/rotateAndPushLogs"
```

Importing a license

To import a license onto an appliance, *license* is used as the action name. You also need to specify a Content-Type header for the type of the license file.

```
curl -i -b cookies.txt -H "Content-Type: text/plain; charset=UTF-8" -X POST "$REST/
appliances/ <UUID>/action/license" --data-binary @license.xml
```

Working with files and lists

When working with system files, log files, files uploaded for troubleshooting, and lists, the *system*, *log*, *files*, and *list* parameters are used in requests instead of the *action* parameter.

Changes made to system files and lists must be commited by sending an appropriate request.

See also

Working with system files on page 318
Working with log files on page 319
Working with files uploaded for troubleshooting on page 320
Working with lists on page 321
Sample scripts for working with the REST interface on page 325

Working with system files

You can use the REST interface to work with system files on an appliance.

Modifying system files in an inappropriate manner can impact the proper operation of an appliance.

In a request to access a system file, for example, the */etc/hosts* file, on a particular appliance, you identify this appliance, using its UUID, and add the *system* parameter to the URL.

If you know the path to a system file and its name, you can include this information in a request to access the file directly.

Otherwise, you can request a feed to deliver a list of the system files that exist on an appliance as follows:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/system"
```

Like with any other feed request, you can also add query parameters for paging to the URL.

With system files, you can do the following:

- Download a system file
- Modify a system file

Unlike with log files and other files on an appliance, you must send a separate request to commit changes you have made to a system file.

When you are running an appliance in FIPS-compliant mode, you cannot modify system files.

Downloading a system file

When downloading a system file, you specify the *application/x-download* Accept header in the request and add the path and name of the system file to the URL.

```
curl -i -b cookies.txt -H "Accept:application/x-download" -X GET "$REST/appliances/
<UUID> /system/etc/hosts" -O
```

The *-O* option stores the data in a local file under the name the file had on the appliance you downloaded it from.

Modifying a system file

When modifying a system file, you set the Content-Type header and add the path and name of the system file to the URL. You also provide a file as the request body containing the data for modifying the system file in binary format.

```
curl -i -b cookies.txt -H "Content-Type: */*" -X PUT "$REST/appliances/<UUID>/system/
etc/hosts" --data-binary @binary.zip
```

Working with log files

You can use the REST interface to work with log files on an appliance.

In a request to access a log file on a particular appliance, you identify this appliance, using its UUID, and add the *log* parameter to the URL.

If you know the path to a log file and its name, you can include this information in a request to access the file directly.

Otherwise, you can request a feed that delivers a list of the files and directories stored in the root log directory on an appliance as follows:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/log"
```

Like with any other feed request, you can also add query parameters for paging to the URL.

The xml file that you receive as a feed in response provides MIME type information to indicate for every element in the feed whether it is an individual log file or a directory.

- *"application/x-download"* — For an individual log file
- *"application/atom+xml; type=feed"* — For a directory

The xml file could, for example, indicate as follows that the root log directory includes the individual log file *debug_1234.log*.

```
<link href="http://localhost:4711/Konfigurator/REST/appliances/
081EEDBC-7978-4611-9B96-CB388EEFC4BC/log/debug/debug_1234.log" rel="self"
type="application/x-download"/>
```

It could also indicate that the directory *connection_tracing* is included, as follows.

```
<link href="http://localhost:4711/Konfigurator/REST/appliances/
081EEDBC-7978-4611-9B96-CB388EEFC4BC/log/debug/connection_tracing" rel="self"
type="application/atom+xml; type=feed"/>
```

Regarding individual log files, you can:

- Download a log file
- Delete a log file

Downloading a log file

When downloading a log file, you specify the *application/x-download* Accept header in the request and add the path and name of the log file to the URL.

```
curl -i -b cookies.txt -H "Accept:application/x-download" -X GET "$REST/appliances/
<UUID> /log/debug/debug_1234.log" -O
```

The *-O* option stores the log file data in a local file under the name it had on the appliance you downloaded it from.

Deleting a log file

When deleting a log file, you add the path and name of the log file to the URL.

```
curl -i -b cookies.txt -X DELETE "$REST/appliances/ <UUID>/log/debug/debug_1234.log"
```

Working with files uploaded for troubleshooting

You can use the REST interface to work with files that have been uploaded for troubleshooting purposes on an appliance.

On the standard user interface of an appliance, you can upload files for troubleshooting purposes under *Files*, which is a location that is accessible from the Troubleshooting top-level menu.

In a request to access one of these uploaded files on a particular appliance, you identify the appliance, using its UUID, and add the *files* parameter to the URL.

If you know the path to an uploaded file and its name, you can include this information in a request to access the file directly.

Otherwise, you can request a feed that delivers a list of these files as follows:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/files"
```

Like with any other feed request, you can also add query parameters for paging to the URL.

You can do the following with the uploaded files:

- Download an uploaded file
- Add a file to the uploaded files
- Modify an uploaded file
- Delete an uploaded file

Downloading an uploaded file

When downloading an uploaded file, you specify the *application/x-download* Accept header in the request and add the name of the file to the URL.

```
curl -i -b cookies.txt -H "Accept:application/x-download" -X GET "$REST/appliances/
<UUID>/files/troubleshooting.zip" -O
```

The *-O* option stores the downloaded data in a local file under the name it had on the appliance you downloaded it from.

Adding a file to the uploaded files

When adding a file to the uploaded files, you set the Content-Type header and add the name of the file to the URL. You also provide this file with data in binary format as the request body.

```
curl -i -b cookies.txt -H "Content-Type: */*" -X PUT "$REST/appliances/<UUID>/files/
moretroubleshooting.zip" --data-binary @moretroubleshooting.zip
```

Make sure that the content type is not *application/x-www-form-urlencoded* , as the curl tool will set the header to this value.

Modifying an uploaded file

When modifying an uploaded file, you set the Content-Type header and add the name of the file to the URL. You also provide a file as the request body containing data for modifying the file in binary format.

```
curl -i -b cookies.txt -H "Content-Type: */*" -X PUT "$REST/appliances/<UUID>/files/
troubleshooting.zip" --data-binary @binary.zip
```

Deleting an uploaded file

When deleting an uploaded file, you add the name of the file to the URL.

```
curl -i -b cookies.txt -X DELETE "$REST/appliances/ <UUID>/files/troubleshooting.zip"
```

Working with lists

You can use the REST interface to work with lists and their entries on an appliance.

In a request to access a list, you add the *list* parameter to the URL.

A request for a feed that delivers a list of all available lists on an appliance could, for example, look as follows:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/list"
```

Like with any other feed request, you can add query parameters for paging to the URL. In addition to this you can add query parameters for the file name and type.

The following request retrieves a feed of all available string lists:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/list?type=string"
```

The following request retrieves a feed of all lists with the name *Default*.

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/list?name=Default"
```

The xml file that you receive as a feed in response to your request provides a list ID for each list. You can use this ID to identify a list that you want to access. A list ID looks, for example, as follows:

```
com.scur.type.regex.11347
```

You can also use the list ID in a request for a feed of the entries in a particular list, together with the *entry* parameter. The following request retrieves a list entry feed:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/list/<list ID>/entry"
```

The xml file that you receive as a feed in response to your request provides a number for each entry to indicate its position. You can use the position to identify an entry that you want to access.

With regard to a list, you can do the following:

- Add a list with content
- Add a list with name and type inside the content
- Add an empty list
- Delete a list
- Retrieve a list
- Modify a list
- Copy a list

With regard to a list entry, you can:

- Retrieve a list entry
- Delete a list entry
- Modify a list entry
- Move a list entry
- Insert a list entry

Adding a list with content

When adding a list with content, you specify the Content-Type header and provide the file in xml format as the request body, using the *-d* option. With the query parameters of the URL, you specify name and type of the list.

```
curl -i -b cookies.txt -H "Content-Type: application/xml" -X POST -d
@listwithcontent.xml "$REST/list?name=newlist&type=category"
```

The response to this request includes the new list in xml format as the response body

The xml file that you send with the request could, for example, look as follows:

```
<entry>
<content type=“application/xml”>
               <list>
               <description/>
               <content>
               <listEntry>
               <entry>com.scur.category.192</entry>
               <description />
               </listEntry>
               <listEntry>
               <entry>com.scur.category.195</entry>
               <description/>
               </listEntry>
               <listEntry>
               <entry>com.scur.category.140</entry>
               <description/>
               </listEntry>
               </content>
               </list>
```

```
</content>
</entry>
```

Adding a list with name and type inside the content

When adding a list that has its name and type included in the content, you specify the Content-Type header and provide the file in xml format as the request body, using the *-d* option.

```
curl -i -b cookies.txt -H "Content-Type: application/xml" -X POST -d
@nameandtypeinside.xml" "$REST/list"
```

The response to this request includes the new list in xml format as the response body.

The xml file that you send with the request could, for example, look as follows:

```
<entry>
<content type=“application/xml”>
           <list name=“Lifestyle” typeId=“com.scur.type.category”>
                 <description/>
                 <content>
                       <listEntry>
                             <entry>com.scur.category.192</entry>
                             <description />
                       </listEntry>
                       <listEntry>
                             <entry>com.scur.category.195</entry>
                             <description/>
                       </listEntry>
                       <listEntry>
                             <entry>com.scur.category.140</entry>
                             <description/>
                       </listEntry>
                 </content>
           </list>
</content>
</entry>
```

Adding an empty list

When adding an empty list, you specify its name and type with the query parameters of the URL.

```
curl -i -b cookies.txt -X POST "$REST/list?name=newlist&type=category"
```

The response to this request includes an empty list in xml format as the response body.

Retrieving a list

When retrieving a list with content, you add its list ID to the URL.

```
curl -i -b cookies.txt -X GET "$REST/list/ <list ID>"
```

The response to this request includes the requested list in xml format as the response body. It has the same structure as a new list that has been added.

Deleting a list

When deleting a list, you add its list ID to the URL.

```
curl -i -b cookies.txt -X DELETE "$REST/list/ <list ID>"
```

Modifying a list

When modifying a list, you replace it with modified content. You specify the Content-Type header and provide the modified content in XML format as the request body, using the *-d* option. You also add the list ID to the URL.

The structure of the modified content is the same as with the content of a list that is added without ilncluding its name and type inside the content.

```
curl -i -b cookies.txt -H "Content-Type: application/xml" -X POST -d @modifiedlist.xml
"$REST/list/<list ID>"
```

The response to this request includes the modified list in xml format as the response body.

Copying a list

When copying a list, you add the ID of the list you want to copy to the URL. You also add the *copy* parameter with a query parameter for the name that the copied list should have.

```
curl -i -b cookies.txt -X POST "$REST/list/<list ID>/copy/?newname"
```

The response to this request includes the modified list in xml format as the response body.

Retrieving a list entry

When retrieving a list entry, you add the list ID and *entry* parameter with the position of the entry to the URL.

```
curl -i -b cookies.txt -X GET "$REST/list/<list ID>/entry/3"
```

The response to this request includes the entry in xml format as the response body.

Deleting a list entry

When deleting a list entry, you add the list ID and *entry* parameter with the position of the entry to the URL.

```
curl -i -b cookies.txt -X DELETE "$REST/list/<list ID>/entry/4"
```

Modifying a list entry

When modifying a list entry, you replace it with modified content. You specify the Content-Type header and provide the modified content in xml format as the request body, using the *-d* option.

You also add the list ID, the *entry* parameter and the position of the entry to the URL.

```
curl -i -b cookies.txt -H "Content-Type: application/xml" -X PUT -d @modifiedentry.xml
"$REST/list/<list ID>/entry/2"
```

The response to this request includes the modified entry in xml format as the response body.

The modified content that you send with the request could, for example, look as follows:

```
<entry xmlns=“http://www.w3org/2011/Atom”>
<content type=“application/xml”>
                                            <listEntry>
                                                <entry>com.scur.category.192</entry>
                                                <description />
                                            </listEntry>
</content>
</entry>
```

Moving a list entry

When moving a list entry, you add the list ID, the *entry* parameter and the old position of the entry to the URL. You also add the *move* and the *newpos* query parameter with the new position.

```
curl -i -b cookies.txt -X POST "$REST/list/<list ID>/entry/4/move?newpos=3"
```

The response to this request includes the entry in xml format with its new position as the response body.

Inserting a list entry

When inserting a list entry, you specify the Content-Type header and provide the entry in xml format a the request body, using the *-d* option.

You also add the iist ID, *entry* parameter, the position where you want to insert the entry, and the *insert* parameter to the URL.

```
curl -i -b cookies.txt -H "Content-Type: application/xml -X POST -d @newentry.xml
"$REST/list/<list ID>/entry/2/insert"
```

The response to this request includes the inserted entry in xml format as the response body.

Sample scripts for working with the REST interface

When working with the REST interface, you can use suitable scripts for sending requests to it.

The following scripts are bash scripts that use curl as the data transfer tool. They complete the following activities:

- Perform an action
- Download a log file
- Create a configuration backup
- Restore a configuration from a backup

Perform an action

The following bash script performs a particular action on each of several appliances.

```
# !bin/bash
# Set URL variable for access to REST interface
REST="http://10.149.112.48:4711/Konfigurator/REST"
```

```
# Set action variable
action="flushcache"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/
login"
## Write appliances feed to appliancesxml variable
appliancesxml=`curl -b cookies.txt "$REST/appliances"`
## Retrieve UUIDs from appliancesxml variable using xpath
uuids=`echo $appliancesxml|xpath -e "/feed/entry/id/text()"``
## Perform action on all appliances, identifying them by their UUIDs
echo $uuids
for uuid in $uuids
do
            echo Sending $action to $uuid
            curl -b cookies.txt -X POST "$REST/appliances/$uuid/action/$action"
done
## Log off again
curl -b cookies.txt -X POST "$REST/logout"
```

Download a log file

The following bash script downloads a particular log file from each of several appliances.

```
# !bin/bash
# Set URL variable for access to REST interface
REST="http://10.149.112.48:4711/Konfigurator/REST"
# Set log file variable
auditlog="/audit/audit.log"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/
login"
## Write appliances feed to appliancesxml variable
appliancesxml=`curl -b cookies.txt "$REST/appliances"`
## Retrieve UUIDs from appliancesxml variable using xpath
uuids=`echo $appliancesxml|xpath -e "/feed/entry/id/text()"`
## Retrieve log file from all appliances, identifying them by their UUIDs
echo $uuids
for uuid in $uuids
do
      echo Downloading $auditlog from $uuid
      curl -b cookies.txt -H "Accept: application/x-download" -X POST "$REST/
      appliances/$uuid/log/$auditlog" -o audit$uuid.log
done
## Log off again
```

```
curl -b cookies.txt -X POST "$REST/logout"
```

Create a configuration backup

The following bash script creates a configuration backup on an appliance.

```
# !bin/bash

# Set URL variable for access to REST interface

REST="http://localhost:4711/Konfigurator/REST"

## Log on and authenticate

curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/
login"

## Create backup file

curl -b cookies.txt -X POST "$REST/backup" -o file.backup

## Log off again

curl -b cookies.txt -X POST "$REST/logout"
```

Restore a configuration

The following bash script restores a configuration from a backup file on an appliance.

```
# !bin/bash

# Set URL variable for access to REST interface

REST="http://localhost:4711/Konfigurator/REST"

## Log on and authenticate

curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/
login"

## Restore configuration from backup file

curl -b cookies.txt --data-binary @file.backup -X POST "$REST/restore" -H
"Content-Type: text/plain; charset=UTF-8"

## Log off again

curl -b cookies.txt -X POST "$REST/logout"
```

17 System tools

When running McAfee Web Gateway on a hardware platform, you can use system tools to complete hardware-related administration activities.

The following tools are available:

- **Platform Confidence Test tool (PCT)** — For running a hardware test
- **Remote Management Module (RMM)** — For administering the hardware remotely
- **Active System Console (ASC)** — For retrieving debugging information about the hardware

You can set up these tools after completing the setup of an appliance.

Contents

System tools for administering the appliance hardware

Several system tools are available for administering the hardware platform that you are running McAfee Web Gateway on.

Platform Confidence Test tool

The Platform Confidence Test (PCT) tool allows you to test the functions of the hardware platform for an appliance. When performing a test, the appliance must not be connected to any network devices.

The test results are stored in the *result.log* file, which you can copy to a USB drive for further use.

Remote Management Module

The Remote Management Module (RMM) enables you to administer hardware functions for an appliance remotely.

Together with this tool, another tool is set up in the same installation procedure. This tool is the Baseboard Management Controller (BMC). It must also be running if you want to use the Active Systeme Console for retrieving debugging information.

Interfaces for the Remote Management Module and the Baseboard Management Controller are located on the rear panel of a McAfee Web Gateway appliance box.

Active System Console

The Active System Console (ASC) is a web-based debugging tool. It provides information on hardware errors involving chassis, storage, cooling, processors, memory, power supply, and other components and functions.

Errors are detected by the Baseboard Management Controller (BMC), which is set up together with the Remote Management Module (RMM). The BMC accesses system event and sensor data records on an appliance.

The Active System Console allows you to configure several BMC functions, such as the IP address or email and trap communication.

The tool also enables you to send hardware data to the McAfee technical support team.

Set up the Platform Confidence Test tool

You can set up the Platform Confidence Test (PCT) to retrieve information on hardware errors.

For each appliance model, there is a particular version of the tool.

Task

1. Download the appropriate tool version from the McAfee Content & Cloud Security Portal.

   Tool versions are available there in zipped format.

2. Extract the content of the downloaded zip file into the root directory of a USB drive that is formatted in Microsoft DOS mode..

3. Attach the USB drive to your appliance.

4. Restart the appliance.

5. When prompted, press **F2** to enter the setup menu.

6. Select **Server Management** | **Console Redirection** and make sure **Console Redirection** is disabled.

7. Select **Boot Manager** and click **EFI Shell**.

   The appliance is restarted in EFI (Extensible Firmware Interface) shell mode.

The EFI shell mode runs the *startup.nsh* procedure from the USB drive and displays a diagnostics menu.

To terminate the diagnostic cycle, press **F10**.

See also

Run a hardware test with the Platform Confidence Test tool on page 330

Run a hardware test with the Platform Confidence Test tool

You can test the appliance hardware using the Platform Confidence Test tool and save the resulting information in a log file.

> **Before you begin**
>
> Make sure the appliance is not connected to any other network component.

Task

1 From the diagnostics menu of the tool, select a test type.

   To test the network interface ports, you can connect any port to another port in the same system using a cross-over cable.

   The test is executed and the result written into a log file on a RAM disk. The name of this log file is *result.log*.

2 Copy the *result.log* file to the USB drive.

   a Run the *map* command.

   b Identify your USB drive in the list that appears. Then enter the following command:

   `cp result.log blk0:` <name of your USB drive>

   In the above command, *blk0* is a device parameter that is required when using a USB drive.

   Different device parameters can be be specified here in some cases.

We recommend that when you have chosen to perform the comprehensive or comprehensive looping test, you do a full AC power cycle (by removing power from the system) before you continue after the test.

This resets all controllers and ensures they are running in an expected mode.

Set up the Remote Management Module

You can set up the Remote Management Module (RMM) to administer the appliance hardware remotely.

Together with this tool, the Baseboard Management Controller (BMC) is set up in the same installation procedure to support the Remote Management Module.

Task

1 Connect the interfaces for the RMM and BMC on the rear panel of an appliance box to the network.

2 Restart the appliance.

3 During the start phase, press **F2**.

   The setup menu appears.

4 Select **Server Management | BMC LAN Configuration**.

5 Under **Baseboard LAN configuration**, configure an IP address, a subnet mask, and a gateway IP address.

6 Under **Intel (R) RMM3 LAN configuration**, configure an IP address, a subnet mask, and a gateway IP address.

7 Under **User configuration**, configure a user name and password to allow an initial user to access the Remote Management Module.

8 Press **F10**, and in the dialog window that appears, click **Yes** to save your changes.

The Remote Management Module is now available for administering the appliance hardware remotely.

You can access the tool through the IP address that you have configured.

The RMM and BMC interfaces are located on the rear panel of an appliance box, together with the network interfaces that are assigned ports for communication with other components of your network.

See also

Port assignments on page 30

Set up the Active System Console

You can set up the Active System Console (ASC) to retrieve debugging information about the appliance hardware.

> **Before you begin**
>
> Make sure the Baseboard Management Controller (BMC) is running, as this is a prerequisite for using the Active System Console.

Task

1. On a system console, run the following command:

   ```
   asc-enable
   ```

2. When prompted, create an administrator password.

   If a message on strong password setting is displayed, respond according to your requirements.

   After the password has been set, the Active System Console is started.

3. Use a web browser to access the ASC user interface under:

   `https://`<IP address of your appliance>`:9393`

When you start the appliance next time, the Active System Console is automatically started with it.

To disable the Active System Console, use the *asc-disable* command.

For more information, see the help information on the ASC user interface and the user documentation that is provided with the hardware platforms.

18 Monitoring

You can monitor an appliance when it executes the filtering that ensures web security for your network.

Monitoring is performed in different ways. Default monitoring on an appliance includes:

- **Dashboard** — Displays key information on the appliance system and activities
- **Logging** — Writes information about important events on an appliance into log files
- **Error handling** — Takes measures when incidents and errors occur on an appliance

You can measure the performance of appliance functions and also use external devices for monitoring, such as a McAfee ePO server or an SNMP Agent.

Contents

Dashboard

The dashboard on the user interface of the appliance allows you to monitor key events and parameters, such as alerts, filtering activities, status, web usage, and system behavior.

Information is provided on the following two tabs:

- **Alerts** — Shows status and alerts
- **Charts and Tables** — Shows web usage, filtering activities, and system behavior

If the appliance is a node in a Central Management configuration, statuses and alerts are also shown for the other nodes.

Access the dashboard

You can access the dashboard on the user interface of an appliance.

Task

1 Select the **Dashboard** top-level menu.

2 Select one of the following two tabs, according to what you want to view:

  - **Alerts** — Shows status and alerts
  - **Charts and Tables** — Shows web usage, filtering activities, and system behavior

See also

View status and alerts information on page 334
View charts and tables information on page 337

Alerts tab

The **Alerts** tab displays information on the status and alerts for an appliance and, in case the appliance is a node in a Central Management configuration, also of the other appliances.

View status and alerts information

On the alerts tab, you can view information on the status of an appliance and on alerts that occur.

Task

1. Select **Dashboard | Alerts**.
2. [Optional] Refresh information on alerts using one of the following two options:
   - **Automatic refresh** — Performs an automatic refresh in regular intervals

     This option is enabled by default.
   - **Refresh now** — Performs an immediate refresh

See also

Overview of status information on page 334
Alert filtering options on page 335

Overview of status information

Information about the status of an appliance is displayed under **Appliances Status** on the **Alerts** tab of the dashboard.

If an appliance is a node in a Central Management configuration, information on the the other nodes is also displayed.

The following table provides an overview of this information.

Table 18-1 Overview of status information

Information	Description
Appliance	Basic appliance information • **Name** — Name of an appliance
Performance	Key performance parameters • **Alert peaks, last 7 days** — Most severe alert on an appliance for each of the last seven days A colored field is displayed for each day (right-most field is today): • Gray — No alert during the day • Green — Most severe alert during the day was an information • Yellow — Most severe alert during the day was a warning • Red — Most severe alert during the day was an error • **Requests per second** — Diagram showing how number of web requests in HTTP and HTTPS mode received on the appliance evolved over the last 30 minutes The value to the right of the diagram is the average number of requests per second over the last ten minutes.

Table 18-1 Overview of status information *(continued)*

Information	Description
McAfee Anti-Malware Versions	Update and version information modules used in virus and malware filtering • **Last update** — Number of minutes since the modules were last updated • **Gateway Engine** — Version number of the McAfee Web Gateway Anti-Malware engine • **Proactive Database** — Version number of the Proactive Database • **DATs** — Version number of the DAT files (containing virus signatures)
URL Filter	Update and version information for the module used in URL filtering • **Last update** — Number of days since the module was last updated • **Version** — Version number of the module

Alert filtering options

Information about alerts on an appliance is provided under **Alerts** on the Alerts tab of the dashboard. You can filter this information using several filtering options.

If an appliance is a node in a Central Management configuration, alerts for the other nodes are also shown. Then you can also filter the nodes you want to view alerts for.

The following table describes the filtering options.

Table 18-2 Alert fiitering options

Option	Definition
Appliance Filter	Filters alerts according to the nodes they occurred on in a Central Management configuration. Clicking this button opens a window for selecting the nodes you want to view alerts for. The filter applies as soon as you close the window.
Date Filter	Filters alerts according to the period of time they occurred in. Clicking this button displays a menu for selecting the time period you want to view alerts for. You can select one of the following: • **All** • **Today** • **Yesterday** • **Last week** • **Custom** Under **Custom**, you can set a start and end date on two calendars and type a start and end time in two filter fields. The time format is hh:mm:ss, using the 24-hours notation, for example, 1 p. m. is 13:00:00. When an appliance is a node in a Central Management configuration and you have selected several nodes of this configuration in the **Appliance Filter**, alerts are shown for these nodes. They are shown, however, according to the date and time shown on the user interface you have been working with on a particular node to set the **Date Filter**. For example, you select *Today* in the **Date Filter** on a node in Amsterdam at 7 p. m. local time. This means all alerts that occurred during the last 19 hours are shown. For a node in New York, local time is 1 p. m. at the time you set the filter. Alerts that occurred on the New York node are then shown for the last 19 hours, not for the last 13 hours, which would correspond to what *Today* is for the New York node.
Message Filter	Filters alerts according to alert message types and strings within the message texts. The filter applies as soon as you have set the filter options. Set these options in the following way: • **Error, Warning, Information** — Select the alert message type you want to view or any combination of types. • **Filter** — Optionally type a filtering term in this field. Only alerts with message texts matching this term and the selected type or types are shown. The search for matching terms is performed on alert entries as they are stored in an internal database on an appliance, not as they appear on the user interface. When alerts appear on the user interface, the alert message text can include additional parts. For example, the word *origin* is added to the name of the component that is the origin of an alert. You can, however, not use *origin* or other added terms to filter alerts.

Charts and Tables tab

The **Charts and Tables** tab displays statistical data on web usage, filtering activities, and system behavior of an appliance. If the appliance is a node in a Central Management configuration, it displays also statistical data for the other nodes.

View charts and tables information

On the **Charts and Tables** tab, you can view information on web usage, filtering activities, and system behavior.

Task

1. Select **Dashboard** | **Charts and Tables**.

2. From the **Appliance** drop-down list, select the appliance you want to view chart and tables information for.

3. [Optional] Click **Update** to ensure you see the most recent information.

4. From the list on the navigation pane, select the type of information you want to view, for example **Web Traffic Summary**.

See also

Charts and tables display options on page 337
Overview of charts and tables information on page 338

Charts and tables display options

There are several options for displaying the information on the Charts and Tables tab, depending on the type of information that is provided.

Types of information are as follows:

- **Evolving data** — Shows how particular parameters evolved over a selected time interval

  For example, you can view how the number of blocked or allowed URL requests evolved over a selected time interval.

- **Top scores** — Shows top numbers for activities or byte volumes related to key items of the filtering process up to the moment when you view them

  What you see then is these numbers, but not how they evolved over time.

  For example, you can view the URL categories that have been most often requested. Or you can view media types ranked according to the volumes transferred when web objects of these types were downloaded.

  The maximum number of items stored on an appliance for presenting top scores at a given point in time is 1500. When this number is exceeded, items that have the lowest occurrence or byte volumes are removed.

- **Other information** — Shows other information presented on tables

  For example, you can view the current versions of key modules (also known as *engines*) on an appliance, such as the Anti-Malware module or the URL Filter module.

The folllowing table shows the display options for the different types of information.

Table 18-3 Charts and tables display options

Option	Definition
Show last	Drop-down list for selecting a time interval: 1 hour | 3 hours | ... | 1 year
Resolution	Displays the time unit used for the diagram that shows the evolution of a parameter over the selected interval. Resolution varies with the interval. For example, when 1 hour is selected, the diagram uses 1 minute as the time unit, when 1 year is selected, the diagram uses 1 day.
View	Drop-down menu for selecting: • Display mode: Line | Stacked • Average values
Refresh icon	Refreshes the view.
Top	Drop-down list for selecting how many of the items with the highest scores are shown: 10 | 25 | ... | 1000 For example, the 25 URL categories that the most often requested URLs fall in can be shown.
Refresh icon	Refreshes the view.

Overview of charts and tables information

Information about web usage, filtering activities, and system behavior for an appliance is displayed on the **Charts and Tables** tab of the dashboard.

The following table provides an overview of this information.

Table 18-4 Executive Summary

Information	Description
URL Executive Summary	Shows how numbers of requests evolved during the interval that was selected for the summary. Requests are sorted into allowed (“good”) requests and such that were blocked by filtering rules for viruses and other malware, URLs, and media types.
Categories by Hits	Shows the URL categories that the most often requested URLs fell in during the selected interval.
Malwares by Hits	Shows the virus and malware types that were requested most often during the selected interval.

Table 18-5 System Summary

Information	Description
Network Utilization	Shows how numbers of requests sent and received evolved during the interval that was selected for the summary.
System Utilization	Shows how usage of hard disk, CPU, physical memory of the appliance system, and the physical memories of the core and coordinator subsystems evolved during the selected interval.
Update Status	Shows the versions of several modules and filter information files that are implemented on an appliance, for example, of the Gateway Antimalware engine or of the malware signature files.
Last Update	Shows when several modules of an appliance were last updated, for example, the URL Filter module.
Open Ports	Lists the ports on an appliance that are currently listening to requests.

Table 18-5 System Summary *(continued)*

Information	Description
WCCP Services	Shows status of WCCP services used to redirect traffic to an appliance.
Active Proxy Connections	Shows how numbers of connections evolved during the selected interval.

Table 18-6 Web Traffic Summary

Information	Description
Traffic per Protocol	Shows how volumes of web traffic under the HTTP, HTTPS, and FTP protocols evolved during the interval that was selected for the summary.
Requests per Protocol	Shows how numbers of requests under the HTTP, HTTPS, and FTP protocols evolved during the selected interval.

Table 18-7 ICAP Traffic Summary

Information	Description
ICAP Traffic	Shows how volumes of ICAP requests in REQMOD and RESPMOD modes evolved during the interval that was selected for the summary.
ICAP Requests	Shows how numbers of ICAP requests in REQMOD and RESPMOD modes evolved during the selected interval.

Table 18-8 IM Traffic Summary

Information	Description
Instant Messaging Traffic	Shows how volumes of instant messaging requests evolved for different services during the interval that was selected for the summary.
Instant Messaging Requests	Shows how numbers of instant messaging requests evolved for different services during the selected interval.
Instant Messaging Clients	Shows how numbers of instant messaging clients evolved for different services during the selected interval.

Table 18-9 Traffic Volume

Information	Description
Top-Level Domains by Bytes Transferred	Lists the domains that were requested most often according to the amount of bytes transferred from them.
Top-Level Domains by Number of Requests	Lists the domains that were requested most according to the number of requests for them.
Destinations by Bytes Transferred	Lists the destinations that were requested most according to the number of bytes transferred from them.
Destinations by Number of Requests	Lists the domains that were requested most according to the number of requests for them.
Source IPs by Bytes Transferred	Lists the source IPs that most volume was transferred to.
Source IPs by Number of Requests	Lists the source IPs that most requests were made from.

Table 18-10 Web Cache Statistics

Information	Description
Web Cache Efficiency	Shows how numbers of caching requests evolved during the interval that was selected for the summary and sorts them into hits and misses.
Web Cache Object Count	Shows how numbers of objects in the cache evolved during the selected interval.
Web Cache Usage	Shows how usage of the cache evolved during the selected interval.

Table 18-11 Malware Statistics

Information	Description
Malware URLs by Hits	Lists the URLs infected by viruses and other malware that were most requested.
Malware by Hits	Lists the malware types that were most requested.

Table 18-12 URL Filter Statistics

Information	Description
Category	Shows how numbers of requested URL categories evolved during the interval that was selected for the summary.
Reputation	Shows how numbers of requests evolved during the selected interval and sorts them according to the reputation of the requested URLs.
Categories by Hits	Lists the URL categories that were most requested
Sites Not Categorized by Hits	Lists among the sites that are not categorized those that were most requested.
Malicious Sites by Hits	Lists among the sites that were found to be infected those that were most requested.

Table 18-13 Media Type Statistics

Information	Description
Media Type Groups by Hits	Shows how numbers of requested media type groups evolved during the interval that was selected for the summary. Types are sorted into audio files, images, and others.
Media Types by Bytes	Lists the media types that were most requested according to the number of bytes transferred.
Media Types by Hits	Lists the media types that were most requested according to the numbers of successful requests for them.

Table 18-14 Certificate Statistics

Information	Description
Certificate Incidents	Shows how numbers of incidents evolved during the interval that was selected for the summary. Incidents are sorted according to the types of the events that caused them, for example, expired certificates or common name mismatches.

Table 18-15 System Details

Information	Description
Network Utilization	Shows how numbers of requests sent and received evolved during the interval that was selected for the summary.
CPU Utilization	Shows how CPU usage evolved during the selected interval.
Memory Usage	Shows how usage of memory evolved during the selected interval.
Swap Space (Virtual Memory) Usage	Shows how usage of virtual memory evolved during the selected interval.
File System Utilization	Shows how usage of the file system evolved during the selected interval.
File System Utilization	Shows usage of the file system per partition during the selected interval.
Open TCP Ports	Shows how numbers of open TCP ports evolved during the selected interval.

Table 18-16 Authentication Statistics

Information	Description
Authentication Requests	Shows how numbers of requests processed remotely, locally, or found in the cache evolved under each authentication method during the interval that was selected for the summary.
Average Request Processing Time per Method in ms	Shows how average processing time for requests sent to a server evolved under each authentication method during the selected interval.
Current Requests Report	Shows numbers of requests, cache hits, and minimum, maximum, and average processing time for requests sent to a server.
Current Connection Status	Shows the connections that are currently active under each authentication method.
File System Utilization	Shows how usage of the file system evolved during the selected interval.
File System Utilization	Shows usage of the file system per partition during the selected interval.
Open TCP Ports	Shows how numbers of open TCP ports evolved during the selected interval.

Table 18-17 Performance Information

Information	Description
General Performance	Shows how the processing time consumed on average for completing particular tasks evolved during the during interval that was selected for the summary. These tasks include performing a DNS lookup, connecting to a given web server, and the work done by the rule engine to process a request throughout all cycles. When measuring the time consumed for DNS lookups, only lookups on external servers are considered. Cache lookups are disregarded.
Detailed Performance	Shows how the time consumed on average for processing a request throughout all cycles evolved during the selected interval. This performance information is only measured and displayed for web traffic that uses HTTP and HTTPS connections. The processing of a request throughout all cycles (request, response, and embedded object cycles) is considered to be one transaction. Average processing time is shown for complete transactions, but also for particular data transfers going on during a transaction: • First Byte Received from Client until First Byte Sent to Client — Shows the average processing time consumed between receiving the first byte from a client on an appliance and sending the first byte to this client within a transaction • Last Byte Received from Client until Last Byte Sent to Client — Shows the average processing time consumed between receiving the last byte received from a client on an appliance on and sending the last byte to this client within a transaction • First Byte Sent to Server until First Byte Received from Sever — Shows the average processing time consumed between sending the first byte from an appliance to a web server and receiving the first byte from this server within a transaction • Last Byte Sent to Server until Last Byte Received from Server — Shows the average processing time consumed between sending the last byte from an appliance to a web server and receiving the last byte from this server within a transaction

Logging

Logging enables you to record web filtering and other processes on an appliance. Reviewing the log files that contain the recordings allows you to find reasons for failures and solve problems.

The following elements are involved in logging:

- Log files that entries recording web filtering and other processes are written into
- System functions that write entries into log files
- Modules that write entries into log files
- Logging rules that write entries into log files
- Log file management modules that rotate, delete, and push log files

Log files

Log files contain entries on web filtering and other processes. Log files with the same kind of content are stored in folders, which are called *logs*. You can view all logs and log files on the user interface of an appliance.

Depending on their content, log files are maintained by functions of the appliance system, modules, or logging rules. Accordingly, you can perform some or all kinds of activities for these log files, such as viewing, editing, rotating, and others.

Logging by system functions

For some content, log file entries are written by functions of the appliance system. You can view these files on the user interface, but not edit or delete them. The files are also rotated in regular intervals by system functions.

Logging by modules

For some content, log file entries are written by particular modules, such as the proxy module or the Anti-Malware module.

You can view these files on the user interface, but not edit or delete them. Rotation and deletion of these files and pushing them to another location is handled by the Log File Manager, which you can configure settings for.

Logging by rules

A logging rule uses events to create a log file entry and write it into a log file if its criteria matches.

Like other rules, logging rules are contained in rule sets. Logging rule sets are nested in top-level rule sets, which are known as *Log Handlers*. A default Log Handler is available after the initial setup of an appliance.

Logging rules are processed in a separate logging cycle after the request, response, and embedded object cycles have been completed for a request that is received on an appliance.

You can work with logging rules and their rule sets in the same way as with other rules and rule sets.

Rotation and deletion of these files and pushing them to another location is handled by the File System Logging module, which you can configure settings for.

Log file management modules

There are two modules for performing management activities on log files, including rotation, deletion, and pushing to other locations.

These modules are the *Log File Manager* for log files that are maintained by modules and the *File System Logging* module (also known as *engine*) for log files maintained by logging rules.

You can configure settings for these modules to adapt the rotation, deletion, and pushing of log files to the requirements of your network.

Administer logging

You can administer the logging functions of an appliance to monitor how it performs filtering and other activities that ensure web security for your network.

Complete the following high-level steps.

Task

1. View the log files that are maintained on an appliance.
2. Modify the implemented log file system as needed.

   You can, for example, do the following:
   - Enable, disable, or delete logging rules
   - Modify logging rules
   - Add logging rules of your own
   - Configure the settings of the logging modules for:
     - Log file rotation
     - Log file pushing
     - Log file deletion
3. Save your changes.

View log files

You can view log files on the user interface of an appliance.

Task

1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to view log files for and click **Log Files**.

   A list of log file folders appears, some of which contain subfolders.
3. Double-click the folder or subfolder with the log files you want to view.

   The folder opens to display its log files.
4. Select the log file you want to view and click **View** on the toolbar above the list.

See also

Log file types on page 343

Log file types

There are several types of log files on an appliance. They differ in the kind of content that is recorded and in the way the recording is done.

Log files that record the same kind of content are stored in the same folder. A folder for storing log files with the same kind of content is called a *log*.

Depending on their content, log files are maintained by system functions, modules, or logging rules.

System-maintained log files

Some log files are maintained by functions of the appliance system, which includes the operating system and several system-related services.

You can view these files on the user interface, but not edit or delete them. However, when system log files are unreadable, they are not displayed on the user interface.

The files are also rotated in regular intervals by system functions. There are no options for configuring this rotation.

Module-maintained log files

Other log files are maintained by particular modules of the appliance, such as the proxy module or the Anti-Malware module.

You can view these files on the user interface, but not edit or delete them. The files are stored in subfolders that are located on the appliance under:

```
/opt/mwg/log
```

Rotation, deletion, and pushing of these files in regular intervals is handled by the Log File Manager, which you can configure settings for.

All files in these folders are handled by the Log File Manager, except those that have *mwgResInfo* as a part of their names.

The folders with the following names are also not handled by the Log File Manager: *cores, feedbacks, tcpdump, migration, system, ruleengine_tracing, connection_tracing, message_tracing*.

Logs for module-maintained log files include the following:

- **Audit log** — Stores log files that record changes to the appliance configuration
- **Debug log** — Stores log files that record debugging information
- **Migration log** — Stores log files that record migration activities
- **MWG errors logs** — Store log files that record errors occurring in appliance components

  There are separate errors logs for the core and coordinator subsystems, the Anti-Malware module, the user interface, and the system configuration daemon.
- **Update log** — Stores log files that record updates of modules and files

Rule-maintained log files

There are also log files that are maintained by logging rules. The recording of data is executed by events that are triggered when these rules apply.

For example, a rule triggers an event when an object that a user requested is infected by a virus. The triggered event writes an entry with information on the user, the infected object, date and time of the request, and other parameters, to the log file.

You can work with the rules for this type of log files in the same way as with any other rules.

Rotation, deletion, and pushing of these files in regular intervals is handled by the File System Logging module, which you can configure settings for.

The following rule-maintained log files are provided on an appliance by default:

- **Access log** — Stores log files that record requests and related information, including date and time, user name, requested object, infection of an object, blocking of an object
- **Found viruses log** — Stores log files that record the names of viruses and other malware that were found to infect requested objects

  The log also records date and time, user name, requested URL, and the IP address of the client a request was sent from.
- **Incident logs** — Store log files that record incidents concerning various functions, such as licensing, monitoring, or updates

To these default logs, you can add logs that you have created yourself.

Configure log file settings

You can configure settings for the log file management modules to modify the way log files are rotated, deleted, and pushed.

The log file management modules handle rotation, deletion, and pushing for module-maintained and rule-maintained log files.

Log file management for system-maintained log files cannot be configured.

Tasks

- *Configure settings for module-maintained log files* on page 345
  You can configure settings for rotation, deletion, and pushing of module-maintained log files. These activities are handled by the Log File Manager.
- *Configure settings for rule-maintained log files* on page 346
  You can configure settings for rotation, deletion, and pushing of rule-maintained log files. These activities are handled by the File System Logging module.

Configure settings for module-maintained log files

You can configure settings for rotation, deletion, and pushing of module-maintained log files. These activities are handled by the Log File Manager.

The settings for module-maintained log files are system settings that are configured for the Log File Manager.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to configure log file settings for and click **Log File Manager**.

   The Log File Manager settings appear on the settings pane.
3. Configure these settings as needed.
4. Click **Save Changes**.

See also
Log File Manager settings on page 346

Configure settings for rule-maintained log files

You can configure settings for rotation, deletion, and pushing of rule-maintained log files. These activities are handled by the File System Logging module.

Task

1. Select **Policy** | **Settings**.
2. On the settings tree, expand **File System Logging** and select the log file settings you want to configure, for example, **Found Viruses Log**.
3. Configure these settings as needed:
4. Click **Save Changes**.

See also
File System Logging settings on page 348

Log File Manager settings

The Log File Manager settings are used for configuring the rotation, deletion, and pushing of log files that are maintained by particular modules of an appliance.

Settings can be configured for log files in general and for two important types of log files, which are stored in the Update Log and the Audit Log.

Global Log File Settings

Settings for log files in general

These settings include options for rotation and deletion of log files and for pushing them to another location.

Auto Rotation

Settings for rotating log files automatically according to their size and the time of day

Table 18-18 Auto Rotation

Option	Definition
Enable auto rotation	When selected, log files are rotated according to the following options. You can configure one of the two options or both.
Enable log file rotation if log file size exceeds	When selected, log files are rotated according to their size (in MiB), as specified in the input field that is provided.
Enable scheduling of log file rotation	When selected, log files are rotated according to the time of day (in hours and minutes), as specified in the input field that is provided. The 24-hours format is used here, for example, 1 p. m. is 13:00.

Auto Deletion

Settings for deleting log files automatically according to their size and the last time of modification

Table 18-19 Auto Deletion

Option	Definition
Enable auto deletion	When selected, log files are deleted according to the following options. You can configure one of the two options or both.
Enable log file deletion if log file size exceeds	When selected, log files are deleted according to their size (in MiB), as specified in the input field that is provided.
Enable autodeletion of unchanged files	When selected, log files are deleted after the period of time (in days) specified in the input field that is provided.

Auto Pushing

Settings for pushing rotated log files automatically to another location

Table 18-20 Auto Pushing

Option	Definition
Enable auto pushing	When selected, rotated log files are pushed from the local database on an appliance to the server that is specified using the following options.
Destination	Network protocol, host name, and path of the server A variable can be added to the path name to specify the pushing process more precisely. For example, *%h* can be added for the host name of the appliance that log files are pushed from. The destination could then be specified as follows: `ftp://myftp.com/%h` When the log files are pushed, the variable is replaced with the appropriate value, which is a host name in this example. The variables you can use here include: • %h — Host name of an appliance • %y — Current year (four digits) • %m — Current month (one or two digits) • %% — Used for specifying the % character (if it is to occur in a host name)
User name	Name of the user who is authorized to push log files to the server The variable *%h* can be specified for the user name. It is replaced by the host name of the current appliance at run time.
Enable pushing log files directly after rotation	When selected, pushing follows rotation immediately.
Push interval	Time (in hours) to elapse before the next log files are pushed if not pushed immediately after rotation

Settings for the Update Log

Specific settings for the Update Log

You can configure these settings if you want them to differ from the global log file settings.

Table 18-21 Settings for the Update Log

Option	Definition
Enable specific update log settings	When selected, the settings configured in the following apply to the Update Log. Otherwise the global log file settings apply.
Auto Rotation, Auto Deletion, Auto Pushing	These settings include the same options and are configured in the same way as the global log file settings.

Settings for the Audit Log

Specific settings for the Audit Log

You can configure these settings if you want them to differ from the global log file settings.

Table 18-22 Settings for the Audit Log

Option	Definition
Enable specific audit log settings	When selected, the settings configured in the following apply to the Audit Log. Otherwise the global log file settings apply.
Auto Rotation, Auto Deletion, Auto Pushing	These settings include the same options and are configured in the same way as the global log file settings.

Advanced

Settings for auto-deletion of core and feedback files

Table 18-23 Advanced

Option	Definition
Enable auto-deletion of core files	When selected, core files are automatically deleted according to the settings you configure. You can specify a number, a time interval, and a volume to let core files that exist in excess of these values be automatically deleted.
Enable auto-deletion of feedback files	When selected, feedback files are automatically deleted according to the settings you configure. You can specify a number, a time interval, and a volume in the same way as for core files.

File System Logging settings

The File System Logging settings are used for configuring the rotation, deletion, and pushing of log files that are maintained by logging rules.

File System Logging Settings

Settings for the log that stores rule-maintained log files

Table 18-24 File System Logging Settings

Option	Definition
Name of the log	Log name
Enable log buffering	When selected, the log is buffered. The buffer interval is 30 seconds.
Enable header writing	When selected, the header below is added to all log files.
Log header	Input field for typing a header for all log files
Encrypt the log file	When selected, log files are stored encrypted.
First password, Repeat password	Input field for creating a password for access to encrypted log files
[Optional] **Second password, Repeat password**	Input field for creating a second password for access to encrypted log files

Settings for Rotation, Deletion, and Pushing

Settings for log file management

The settings for rotating, deleting, and pushing rule-maintained log files include the same options and are configured in the same way as the corresponding settings for module-maintained log files, which are configured as part of the Log File Manager settings.

See also
Log File Manager settings on page 346

Create a log

You can create a log that can be used by a logging rule to write entries into its log files.

When you create a log, you do not create it separately, but as a part of creating new settings for the File System Settings module.

Task

1. Select **Policy** | **Settings**.
2. Expand **File System Logging** and select one of the existing settings, for example, **Access Log Configuration**.

   This will serve as a starting point for creating new settings, including the creation of a new log.
3. Click **Add** above the settings tree.

   The **Add Settings** window opens.
4. In the **Name** field, type a name for the settings.
5. [Optional] In the **Comment** field, type a plain-text comment on the settings.
6. [Optional] Select the **Permission** tab and configure who is allowed to access the settings.
7. Under **Name of the log**, type the name of the new log.
8. Configure other settings items, such as rotation or deletion, as needed.
9. Click **OK**.

   The **Add Settings** window closes and the new settings appear under **File System Logging** on the settings tree.
10. Click **Save Changes**.

Create a log handler

When you create new logging rules, you can insert them into existing logging rule sets or create new rule sets for them. These must be nested themselves in top-level rule sets known as log handlers.

You can also use the Default log handler for inserting new logging rule sets.

Task

1 Select **Policy** | **Rule Sets**.

2 From the **Rule Sets** menu, select **Log Handler**.

3 Click **Add** above the log handler tree, and from the drop-down menu that appears, select **Log Handler**.

   The **Add New Log Handler** window opens.

4 In the **Name** field, type a name for the log handler.

5 Make sure **Enable** is selected.

6 [Optional] In the **Comment** field, type a plain-text comment on the log handler.

7 [Optional] Click the **Permissions** tab and configure who is allowed to access the log handler.

8 Click **OK** to close the **Add New Log Handler** window.

   The new log handler appears on the log handler tree.

9 Click **Save Changes**.

Elements of a logging rule

A logging rule handles the writing of log file entries into a particular log. Its elements are of the same types as with other rules.

Name

Write Found Viruses Log

Criteria		Action		Events
Antimalware.Infected equals true	–>	Continue	–	Set User-Defined.LogLine = + DateTime.ToWebReporterString + “ ”” + Authentication.Username + “ ” + String.ReplaceIf Equals (IP.ToString(Client.IP), “””, “-”) + ““ ”” + List.OfString.ToString (Antimalware.VirusNames) + ““ ”” + URL + “““ FileSystemLogging.WriteLogEntry (User-Defined.logLine)<Found Viruses Log>

The elements of this rule have the following meanings:

- **Criteria** — *Antimalware.Infected equals true*

  The criteria of the rule uses the *Antimalware.Infected* property. It is matched when the value of this property is *true*. This means that the rule applies when a filtered object is infected.

- **Action** — Continue

  When the rule applies, it executes the the Continue action. This action lets processing continue with the next rule after the events of the current rule have also been executed.

- **Events** — When the rule applies, it also executes two events:

  - **Set User-Defined.logLine = ...** — Sets the parameter values that are logged.

    Theses values are as follows:

  - **FileSystemLogging.WriteLogEntry ...** — Executes the write event

    The entry that is to be written and the log file it is written into are specified with the event:

    - (User-Defined.logLine) — Event parameter specifying the entry

      This is a log file line with the parameter values that have been set by the other event of the rule.

    - <Found Viruses Log> — Event settings specifying the log file

Access log rule set

The Access Log rule set is a nested rule set in the Default Log Handler rule set.

Nested default rule set – Access Log
Criteria – *Always*

The rule set contains the following rule.

Write access.log

Always –> Continue —

Set User-Defined.logLine = DateTime.ToWebReporterString + ‟ ”” ...

FileSystemLogging.WriteLogEntry (User-Defined.logLine)<Access Log Configuration>

The rule uses an event to fill a log file entry with parameter values relating to requests sent by users, such as user names or request headers.

It uses another event to write this entry into a log file.

The log file entry is specified as a parameter in both events. The log that stores the log file is specified by the settings of the write event.

Values for the following parameters are set and logged by the events of the rule (properties used by the event that sets the values are shown in italics):

- Date and time — *DateTime.ToWebReporterString*
- User name — *Authentication.UserName*
- Client IP address — *String.ReplaceIfEquals (IP.ToString(Client.IP), "", "-")*
- Response status — *String.ReplaceIfEquals (Number.ToString (Response.StatusCode), "", "-")*
- Request header — *RequestHeader.FirstLine*
- URL category — *List.OfCategory.ToString (URL.Categories)*
- URL reputation — *String.ReplaceIfEquals (URL.ReputationString, "", "-") (URL.Reputation<Default>)*
- Media type — *MediaType.ToString (MediaType.FromHeader)*
- Body size — *String.ReplaceIfEquals (Number.ToString (Body.Size), "", "-")*
- User agent — *Header.Request.Get("User-Agent")*
- Virus and malware names — *List.OfString.ToString (Antimalware.VirusNames)*
- Block action ID — *Number.ToString (Block.ID)*

The logging rule applies whenever a request for access to the web is received.

The two rule events for filling and writing a log entry are then executed.

Processing continues with the next rule or rule set.

Found Viruses Log rule set

The Found Viruses Log rule set is a nested rule set in the Default log handler rule set.

Nested default rule set – Found Viruses Log
Criteria – *Always*

The rule set contains the following rule.

Write found viruses.log

Antimalware.Infected equals true –> Continue —

Set User-Defined.logLine = DateTime.ToWebReporterString + " "" ...

FileSystemLogging.WriteLogEntry (User-Defined.logLine)<Found Viruses Log>

The rule uses an event to fill a log file entry with parameter values relating to web objects that are infected by viruses or other malware, such as virus names or IP addresses.

It uses another event to write this entry into a log file.

The log file entry is specified as a parameter in both events. The log that stores the log file is specified by the settings of the write event.

Values for the following parameters are set and logged by the events of the rule (properties used by the set event are shown in italics):

- Date and time — *DateTime.ToWebReporterString*
- User name — *Authentication.UserName*
- Client IP address — *String.ReplaceIfEquals (IP.ToString(Client.IP), "", "-")*
- Virus and malware names — *List.OfString.ToString (Antimalware.VirusNames)*
- URL — *URL*

The logging rule applies whenever a requested web object has been found to be infected. The two rule events for filling and writing a log entry are then executed.

Processing continues with the next rule or rule set.

Error handling

When errors and incidents occur on an appliance, appropriate measures can be taken. Some of these measures are controlled by rules.

Error handling using error IDs

Errors that occur on an appliance are identified by error IDs. These can be used by rules to trigger particular methods of error handling.

To enable the use of error IDs in rules, the *Error.ID* property is available. A rule can trigger an action or event when this property has a particular value, for example, 14000, which indicates a failure to load the Anti-Malware module.

The action or event that is triggered uses a particular method of error handling, such as blocking access to a web object or creating an entry in a log file.

A rule that uses an error ID to trigger an error handling measure could, for example, look at follows

Name

Block if Anti-Malware engine cannot be loaded

Criteria		Action
Error.ID equals 14000	–>	Block<Cannot Load Anti-Malware Engine>

Error handling using incident information

There is a group of activities and situations on an appliance that is termed *incidents*. Incident information can be used by rules to trigger particular methods of error handling.

Incidents can be related to the appliance system, as well as to its subsystems and modules. For example, a failure of the Log File Manager to push log files is recorded as an incident.

Incidents can be used by rules to trigger a particular method of error handling, such as sending a notification message or creating an entry in the system log. To enable the use of incidents in rules, key incident parameters, including the ID, severity, origin, and others, are made available as properties.

For example, there is the *Incident.ID* property. A rule can use this property to trigger an event that creates a syslog entry if the value of the property is a particular number.

Rules using incidents

The Default rule set for error handling contains a nested rule set providing rules that trigger a notification message and other error handling events when incidents concerning the Log File Manager occur. The name of this nested rule set is Log File Manager Incidents. Other nested rule sets handle incidents related to updates and licensing.

You can also create rules and rules sets of your own that use incidents for error handling.

Incident parameters and properties

Incidents are recorded on an appliance with their IDs and other parameters. For each parameter, there is a property, which can be used in an appropriate rule.

- **Incident ID** — Each incident is identified by a number. For example, the incident with ID 501 is a failure of the Log File Manager to push log files. The *Incident.ID* property can be used in a rule to check the ID of an incident.
- **Description** — An incident can be explained by a description in plain text. The name of the relevant property is *Incident.Description*.
- **Origin** — Each incident is assigned to the appliance component that is its origin. Origins are specified by numbers. For example, origin number 5 specifies the Log File Handler. The name of the relevant property is *Incident.Origin.*
- **OriginName** — The origin of an incident is further specified by the name of the appliance component that is involved in the incident. The name of the relevant property is *Incident.OriginName*.

  The origin name can specify a subcomponent that is a part of the component specified by the origin number. For example, origin number 2 (Core) can be further specified by the origin name as:
  - Core
  - Proxy
  - URL Filter
  - and other names of core subcomponents
- **Severity** — Each incident is classified according to its severity. Severity levels range from 0 to 7, with 0 indicating the highest level.

  These levels are the same as those used for entries in a syslog file.

  The name of the relevant property is *Incident.Severity*.
- **Affected host** — If there is an external system that is involved in an incident, for example, a server that the appliance cannot connect to, the IP address of this system is also recorded. The name of the relevant property is *Incident.AffectedHost*.

Configure error handling

You can configure error handling to adapt this process to the requirements of your network.

Complete the following high-level steps.

Task

1. Review the rules in the nested rule sets of the default rule set for error handling.

   The name of this rule set is *Default*.
2. Modify these rules as needed.

   You can, for example, do the following:
   - Enable rules that take additional measures for error handling when a particular error or incident has occurred.
   - Create new rules and rule sets for handling additional errors and incidents.
3. Save your changes.

View the error handling rule sets

You can view the rule sets that are implemented for error handling on a rule set tree that is provided on the user interface in addition to the normal rule set tree for web filtering rules.

Task

1. Select **Policy | Rule Sets**.
2. Below the rule sets tree, select **Error Handler**.
3. Expand the **Default** top-level rule set.

   The nested rule sets for error handling appear.
4. Select a nested rule set.

   The rules of the nested rule set appear on the settings pane.

See also

Default error handler rule set on page 355

Default error handler rule set

The Default error handler rule set is the default rule set for error handling.

Default error handler rule set – Default
Criteria – *Always*

The following rule sets are nested in this rule set:

- Long Running Connections
- Monitoring
  - Check CPU Overload
  - Check Cache Partition
  - Check Request Overload
- Log File Manager Incidents
- Handle Update Incidents
- Handle License Incidents
- Block on Antimalware Engine Errors
- Block on URL Filter Errors
- Block on All Errors

Long Running Connections

This nested error handler rule set keeps connections alive when a proxy module error occurs.

Nested error handler rule set – Long Running Connections
Criteria – *Error.ID equals 20000*

The rule set criteria specifies that the rule set applies when the value of the Error.ID property is 20000, which indicates a malfunction of the proxy module.

The rule set contains the following rule.

Keep connection always alive

Always –> Stop Cycle

When the rule is executed, it stops the current processing cycle. The rule is always executed when the criteria of its rule set is matched. Stopping the processing cycle prevents the connection from being closed in the course of further rule processing.

The rule is not enabled by default.

Monitoring

This nested error handler rule set handles measures taken when an incident occurs that involves the appliance system.

Nested error handler rule set – Monitoring
Criteria – *Incident.ID equals 5*

The rule set criteria specifies that the rule set applies when the value of the Incident.ID property is 5, which indicates an incident that involves the appliance system.

The following rule sets are nested in this rule set:

- Check CPU Overload
- Check Cache Partition
- Check Request Overload

Check CPU Overload

This nested error handler rule set handles measures that are taken when the CPU load exceeds a configured value.

Nested error handler rule set – Check CPU Overload
Criteria – *Statistics.Counter.GetCurrent("CPULoad")<Default> greater than or equals 95*

The rule set criteria specifies that the rule set applies when the value of the Statistics.Counter. GetCurrent property for CPU load is 95 or higher. This value indicates the percentage of the maximum load that the CPU is currently running with.

The Statistics module, which provides the value, runs with default settings, as is specified after the CPU Load property parameter.

The rule set contains the following rules.

Create notification message

Always –> Continue – Set User-Defined.loadMessage =

"CPU load at "

+ Number.ToString (Statistics.Counter.GetCurrent("CPULoad")<Default>)

+ "%"

The rule is always executed when the criteria of its rule set is matched.

The rule then uses an event to set a user-defined property to a chain of values that make up a message text about the CPU overload.

The Continue action lets processing continue with the next rule.

Send SNMP trap and other rules

Always –> Continue – ...

The Send SNMP trap rule and other rules in the rule set are always executed when the rule set criteria is matched.

The rules then use different events for taking measures to make the administrator aware of the CPU overload.

These rules are not enabled by default.

Check Cache Partition

This nested error handler rule set handles measures that are taken when the web cache usage exceeds a configured value.

Nested error handler rule set – Check Cache Partition
Criteria – *Statistics.Counter.GetCurrent("WebCacheDiskUsage")<Default> greater than or equals 95*

The rule set criteria specifies that the rule set applies when the value of the Statistics.Counter. GetCurrent property for web cache usage is 95 or higher.This value indicates the percentage of the maximum allowed usage of the web cache that is currently in use.

The Statistics module, which provides the value, runs with default settings, as is specified after the WebCacheDiskUsage property parameter.

The rule set contains the following rules.

Create notification message

Always –> Continue – Set User-Defined.cacheMessage =

"Cache partition usage at "

+Number.ToString (Statistics.Counter.GetCurrent("WebCacheDiskUsage")<Default>)

+ "%"

The rule is always executed when the criteria of its rule set is matched.

The rule then uses two events to set user-defined properties. One of these properties is set to the number of requests that are currently processed on the appliance per second. The other is set to a chain of values that make up a message text about the web cache usage..

The Continue action lets processing continue with the next rule.

Send SNMP trap and other rules

Always –> Continue – ...

The Send SNMP trap rule and other rules in the rule set are always executed when the rule set criteria is matched.

The rules then use different events for taking measures to make the administrator aware of the web cache usage.

These rules are not enabled by default.

Check Request Overload

This nested error handler rule set handles measures that are taken when the number of requests processed on an appliance per second exceeds a configured value.

Nested error handler rule set – Check Request Overload
Criteria – *Statistics.Counter.GetCurrent("HttpRequests")<Default> greater than or equals 480000*

The rule set criteria specifies that the rule set applies when the value of the Statistics.Counter. GetCurrent property for requests is 480,000 or higher. This value is the number of requests that are currently processed one an appliance per second.

The Statistics module, which provides the value, runs with default settings, as is specified after the HttpRequests property parameter.

The rule set contains the following rules.

Create notification message

Always –> Continue – Set User-Defined.requestsPerSecond =

Statistics.Counter.GetCurrent("HttpRequests")<Default>)

/ 60

Set User-Defined.requestLoadMessage =

"detected high load: "

+ Number.ToString (User-Defined.requestsPerSecond)

+ "requests per second"

The rule is always executed when the criteria of its rule set is matched.

The rule then uses two events to set user-defined properties. One of these properties is set to the number of requests that are currently processed on an appliance per second. The other is set to a chain of values that make up a message text about this number.

The Continue action lets processing continue with the next rule.

Send SNMP trap and other rules

Always –> Continue – ...

The Send SNMP trap rule and other rules in the rule set are always executed when the rule set criteria is matched.

The rules then use different events for taking measures to make the administrator aware of the request overload.

These rules are not enabled by default.

Log File Manager Incidents

This nested error handler rule set handles measures taken when an incident occurs that involves the Log File Manager.

Nested error handler rule set – Log File Manager Incidents
Criteria – *Incident.ID greater than or equals 501 AND Incident ID less than or equals 600*

The rule set criteria specifies that the rule set applies when the value of the Incident.ID property is within the range of incidents that involve the Log File Manager.

The rule set contains the following rules.

Create notification message

Incident.ID equals 501 –> Continue – Set User-Defined.notificationMessage =

"License expires in "

+ Number.ToString (License.RemainingDays)

+ " days"

The rule is always executed when the criteria of its rule set is matched.

The rule then uses an event to set a user-defined property to a chain of values that make up a message text on the remaining number of days for your license.

The Continue action lets processing continue with the next rule.

Create syslog entry

Always –> Continue – ...

The Create syslog entry rule and other rules in the rule set check the value of the Incident.ID property in the same way as the Create notification message rule and use different events to take measures if this value is 501.

These rules are not enabled by default.

Handle Update Incidents

This nested error handler rule set handles measures taken when an incident occurs that involves the Log File Manager.

Nested error handler rule set – Handle Update Incidents
Criteria – *IIncident.OriginName equals "Updater" OR Incident.ID equals 850 OR Incident.ID equals 851 OR Incident.ID equals 940 OR Incident.ID equals 941 OR Incident.ID equals 1050 OR Incident.ID equals 1051 OR Incident.ID equals 1650 OR Incident.ID equals 1651*

The rule set criteria specifies that the rule set applies when the update module is specified by the value of the Incident.OriginName property or the value of the Incident.ID property is one of those hat involve the update module.

The rule set contains the following rules.

Create update incident message

Always –> Continue – Set User-Defined.eventMessage =

"Update Event triggered ["

+ Number.ToString (Incident.ID)

+ "]:"

+ Incident.Description

+ "; origin:"

+ Incident.OriginNamey

+ "; severity:"

+ Number.ToString (Incident.Severity)

The rule is always executed when the criteria of its rule set is matched.

The rule then uses an event to set a user-defined property to a chain of values that make up a message text about the update incident. The message includes values for several incident properties.

The Continue action lets processing continue with the next rule.

Create syslog entry

Always –> Continue – ...

The Create syslog entry rule and other rules in the rule set use different events to take measures if the respective rule criteria is matched.

These rules are not enabled by default.

Handle License Incidents

This nested error handler rule set handles measures taken when an incident occurs that involves the expiration date of the license for your appliance.

Nested error handler rule set – Handle License Incidents
Criteria – *Incident.ID equals 200*

The rule set criteria specifies that the rule set applies when the value of the Incident.ID property is 200, which indicates that the remaining number of days for your licence has been checked.

The rule set contains the following rules.

Create license incident message

Always –> Continue – Set User-Defined.notificationMessage =

“A log file cannot be pushed. Please have a look at the mwg-logfilemanager errors log (/opt/mwg/log/mwg-errors/mwg-logmanager.errors.log).”

The rule checks whether the value of the Incident.ID property is 501, which indicates that the Log File manager could not push a log file.

If this is the case, the rule uses an event to set a user-defined property for sending a notification message to a string value that is the text of this message.

The Continue action lets processing continue with the next rule.

Create syslog entry

Always –> Continue – ...

The Create syslog entry rule and other rules in the rule set use different events to take measures if the respective rule criteria is matched.

These rules are not enabled by default.

Block on Anti-Malware Errors

This nested error handler rule set blocks access to all web objects when the Anti-Malware module cannot be loaded or is overloaded.

Nested error handler rule set – Block on Anti-Malware Errors
Criteria – *Always*

The rule set contains the following rules.

Block if Anti-Malware engine cannot be loaded

Error.ID equals 14000 –> Block<Cannot Load Anti-Malware>

The rule blocks access to all web objects when the value of the Error.ID property is 14000, which indicates an error that prevents the Anti-Malware module (also known as *engine*) from loading.

The action settings specify a message to a requesting user.

Block if Anti-Malware engine is overloaded

Error.ID equals 14001 –> Block<Anti-Malware Engine Overloaded>

The rule blocks access to all web objects when the value of the Error.ID property is 14001, which indicates all connections to the Anti-Malware module (also known as *engine*) are currently in use and the module is overloaded.

The action settings specify a message to a requesting user.

Block on URL Filter Errors

This nested error handler rule set blocks access to all web objects when the URL Filter module cannot be loaded or another error regarding this module occurs.

Nested error handler rule set – Block on URL Filter Errors
Criteria – *Error.ID greater than or equals 15000 AND Error.ID less than or equals 15999*

The rule set criteria specifies that the rule set applies when the value of the Error.ID property lies within the specified range, which is the range for errors related to URL filtering.

The rule set contains the following rules.

Block if the URL Filter engine cannot be loaded

Error.ID equals 15000 OR Error.ID equals 15002 OR Error.ID equals 15004 OR Error.ID equals15005 –> Block<Cannot Load URL Filter>

The rule blocks all requests for web access when the value of the Error.ID property is one of those specified in the rule criteria. These values indicate errors that prevent the URL Filter module (also known as *engine*) from loading.

The action settings specify a message to a requesting user.

Block all other internal URL Filter errors

Always –> Block<Internal URL Filter Error>

The rule is always executed when its rule set applies and the rule preceding it in the rule set has not been executed. The rule then blocks all requests for web access.

The action settings specify a message to a requesting user.

Block on All Errors

This nested error handler rule set blocks access to all web objects when an internal error occurs on the appliance.

Nested error handler rule set – Block on All Errors
Criteria – *Always*

The rule set contains the following rule.

Always block

Always –> Block<Internal Error>

The rule blocks access to all web objects when an internal error occurs.

The action settings specify a message to a user who requested access.

The rule in this rule set is for handling internal errors on the appliance. It is executed at the time when an internal error occurs, which can, of course, not be predicted and can happen at any time during the filtering process or not at all. In this sense, processing the rule is not part of the normal process flow.

After executing the blocking, the rule stops all further processing of rules for the requests,responses, or embedded objects that were being filtered when the internal error occurred.

This way it is ensured that no malicious or inappropriate web objects enter your network or leave it while the appliance is not fully available.

The process flow continues when the next request is received if the internal error did not lead to a general interruption of the appliance functions.

Performance measurement

Processing time for several appliance functions is measured and shown as performance information on the dashboard. You can record this information in log files and also measure and record processing time for individual rule sets.

Performance is measured on aan appliance, for example, with regard to the average time it takes to resolve host names by looking up names on a DNS server. You can view this and other performance information on the dashboard. Additionally, you can measure the time needed for processing individual rule sets.

You can also log all performance information, the one shown on the dashboard and the one you have measured yourself.

The following elements are involved when you measure and log performance information:

- Properties for logging performance information
- Logging rules that use these properties to log performance information
- Events that measure processing time for individual rule sets
- Rule sets that include rules with events to have their processing time measured

Logging properties

Several properties are available that correspond to performance information shown on the dashboard and can be used in logging rules.

For example, the property*Timer.ResolveHostNameViaDNS* corresponds to the dashboard information on the average time for looking up host name names on a DNS server.

Two properties are available for logging the time that has been measured for processing an individual rule set. The *Stopwatch.GetMilliSeconds* property records this time in milliseconds, the *Stopwatch.GetMicroSeconds* records it in microseconds.

Logging rules

The default logging rules on an appliance use one event to create log lines and another to write these lines into a log file.

If you add properties for logging performance information to the elements of the log lines, they are written into the log file together with the other elements of the log line.

You can use default rules for logging performance information or create rules of your own.

Events for measuring processing time

Two events are available for measuring the time consumed for processing individual rule sets. The *Stopwatch.Start* event starts the internal stopwatch that measures this time. The *Stopwatch.Stop* event stops the watch, so the time that has elapsed can be recorded.

Measured rule sets

To measure the time consumed for processing a particular rule set, you need to create a rule with the event for starting the internal stopwatch at the beginning of the rule set and another at the end with the stopping event.

You need to insert the stopping event also into existing rules of the rule set if they have actions that stop processing of the rule set. Otherwise, the watch would not be stopped because the rule with the stopping event at the end of the rule set is skipped.

View performance information

You can view performance information about several appliance functions on the dashboard.

Task

1. Select **Dashboard | Charts and Tables**.
2. Select **Performance Information**.

   Performance information appears on the tab.

See also

Overview of charts and tables information on page 338

Configure performance measurement

You can configure performance measurement to measure and log the performance of functions on an appliance.

Complete the following high-level steps.

Task

1. View the performance information shown on the dashboard and decide what kind of information you want to record in a log file.

   For example, you might want to record the average time consumed for looking up host names on a DNS server. This information is shown by the *DNS Lookup* feature of the dashboard.

2. Use the properties that are available for logging performance information in existing logging rules or new logging rules that you create.

   For example, insert the *Timer.ResolveHostNameviaDNS* property into the event that creates a log line in the *Write access.log* rule of the default *Access Log* rule set.

3. Measure the time consumed for processing particular rule sets.

   a. Insert a rule with an event that starts the internal stopwatch at the beginning of a rule set.

   b. To stop the watch and measure the time consumed:

      - Insert a rule with an event that performs these activities at the end of the rule set.
      - Insert an event that performs these activities into each of the existing rules that is capable of stopping the rule set before all its rules are processed.

   For example, to measure the processing time consumed by a URL filtering rule set:

   - insert a rule with the *Stopwatch.Start (URL Filtering)* event at the beginning of the rule set.
   - Insert a rule with the *Stopwatch.Stop (URL Filtering)* event at the end.
   - Insert the *Stopwatch.Stop (URL Filtering)* event into each of the whitelisting and blocking rules of the rule set because they all can stop the processing of further rules.

4. Use the properties that are available for logging the measured processing time in existing logging rules or new logging rules that you create.

   For example, insert the *Stopwatch.GetMilliSeconds (URL Filtering)* property into the event that creates a log line in the *Write access.log* rule of the default *Access Log* rule set.

Using properties in rules to log performance information

You can insert performance logging properties into logging rules to let performance information be logged.

For each type of performance information that is shown on the dashboard, a logging property is available.

For example, the dashboard shows the average time it takes to resolve host names by looking up names on a DNS server. The property *Timer.ResolveHostNameViaDNS* corresponds to this information. The value of the property is the time consumed for looking up a host name in a request that was processed on an appliance. The time is measured in milliseconds.

Other performance logging properties are*Timer.HandleConnect ToServer* for measuring the time needed to connect to external servers or *Timer.TimeConsumedByRule Engine* or the time the rule engine consumes for processing when a request is received on an appliance.

All properties that make dashboard performance information available for logging have the element *Timer* at the beginning of their names.

Measuring processing time for a transaction

The time that is measured and made available by a property for logging performance information shown on the dashboard is the time needed for a particular activity, for example, connecting to external servers, as long as processing for an individual request is continued throughout the relevant processing cycles.

Processing one individual request throughout the relevant cycles is considered one *transaction*.

It is not required for a transaction to include all three cycles (request, response, and embedded objects).

For example, if a user sends a request for a web page that falls into a blocked category, a block message is returned to this user, the request is not forwarded to the web server in question, and processing does not enter the response cycle.

Then the transaction includes only the request cycle, the response cycle is not relevant in this case.

Rule for logging performance information

An Access Log exists by default on an appliance with log files into which a log entry is written whenever a transaction has been completed for a request. This log is an appropriate device for recording performance information.

Writing log entries into the log files of the Access Log is performed by a logging rule. This rule uses one event to create a log file entry and another to write this entry into a log file.

Name

Write access.log

Criteria		Action		Events
Always	–>	Continue	–	Set User-Defined.logLine = DateTime.ToWebReporterString + “”” + ... FileSystemLogging.WriteLogEntry (User-Defined.logLine)<Access Log Configuration>

A log entry is composed of several elements, each of which adds a particular piece of information, for example, the date and time when a request was received on the appliance. By adding an element providing performance information to the entry you can let this information be logged.

To log performance information, for example, on the processing time consumed by DNS lookups, you need to add the following two elements:

- `+ Number.ToString (Timer.ResolveHostNameViaDNS)`
- + “””

Since the log entry is a string, the numerical value for the processing time must be converted to string format before it can be logged.

This is done by the *Number.ToString* property, which takes the *Timer.ResolveHostNameViaDNS* property as a parameter.

Using events in rules to measure rule set processing time

You can measure the time it takes to process an individual rule set by inserting rules with measuring events into it.

The reason for measuring processing time could be that you want to know whether performance is improved or reduced after you have applied changes to a rule set.

The events for measuring rule set processing time control an internal stopwatch on an appliance. The following events are available:

- **Stopwatch.Start** — Starts the internal stopwatch
- **Stopwatch.Stop** — Stops the watch
- **Stopwatch.Reset** — Resets the watch

Each of these events takes a string parameter to indicate which rule set it measures. For example, an event that starts the internal watch to measure the processing time of the URL Filtering rule set, would appear in a rule as follows: *Stopwatch.Start ("URLFiltering")*.

Rules for measuring processing time

A rule that uses, for example, the *Stopwatch.Start* event to start measuring processing time for the URL Filtering rule set could look as follows:

Name

Start stopwatch for rule set

Criteria		Action		Event
Always	–>	Continue	–	Stopwatch.Start (“URLFiltering”)

To measure the time consumed for processing the rule set, you need to place a rule with the starting event at the beginning of the rule set and another one that contains the stopping event at the end.

However, if you have rules in a rule set that can execute a Stop Rule Set, Stop Cycle, or Block action, you also need to insert a stopping event into each of these rules.

A URL filtering rule with an event to stop the internal watch inserted would look as follows:

Name

Allow URLs in URL Whitelist

Criteria		Action		Event
URL matches in URL Whitelist	–>	Continue	–	Stopwatch.Stop (“URLFiltering”)

When this rule is applied, it stops processing the URL Filtering rule set because the URL that a user requested access for has been found to be on the list of allowed URLs.The stopping event must therefore be inserted into this rule.

This is required because the rule with the stopping event at the end of the rule set is then not processed as the whitelisting rule stops processing of the rule set before this rule is reached.

Logging measured processing time

You can log the time that has been measured for rule set processing. Two properties are available for this purpose, which you can use in logging rules.

- **Stopwatch.GetMilliSeconds** — Time measured for rule set processing in milliseconds
- **Stopwatch.GetMicroSeconds** — Time measured for rule set processing in microseconds

Both properties have a string parameter, which indicates the rule set that processing time was measured for.

For example, a property for logging the processing time of the URL Filtering rule set in milliseconds would appear in a logging rule as follows: *Stopwatch.GetMilliSeconds ("URL Filtering")*.

Transferring data for McAfee ePO monitoring

Transferring data from an appliance to the McAfee ePolicy Orchestrator® (McAfee ePO™) console allows you to monitor the appliance from the console.

The McAfee ePolicy Orchestrator console is a device for performing security management on different McAfee products, including the McAfee Web Gateway appliance.

If you configure the McAfee ePO console and an appliance accordingly, you can log on to the appliance from the console and have monitoring data transferred from the appliance to the server that the console is running on. This server is also referred to as the McAfee ePO server.

The McAfee ePO server sends SSL-secured requests to retrieve the monitoring data that has been collected on the appliance in regular intervals. Then you need to allow the CONNECT request that the SSL-secured communication begins with to bypass the normal processing of web security rules, so it does not get blocked on the appliance.

For example, if you have authentication rules implemented, this would lead to blocking because the server does not support the authentication method used by these rules.

You can import an appropriate rule set from the library to enable the bypassing or create a rule set of your own.

Configure the ePolicy Orchestrator settings

You can configure the ePolicy Orchestrator settings to enable the transfer of monitoring data from an appliance to a McAfee ePO server.

Task

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to transfer monitoring data from and click **ePolicy Orchestrator**.

3 Configure the ePolicy Orchestrator settings as needed.

4 Click **Save Changes**.

See also
ePolicy Orchestrator settings on page 367

ePolicy Orchestrator settings

The ePolicy Orchestrator settings are used for configuring the transfer of monitoring data from an appliance to a McAfee ePO server.

ePolicy Orchestrator Settings

Settings for transferring monitoring data to a McAfee ePO server

Table 18-25 ePolicy Orchestrator Settings

Option	Definition
ePO user account	User name for the account that allows the retrieval of monitoring data from an appliance
Password	Password for the user
Change	Opens a window to create a new password.
Enable data collection for ePO	When selected, monitoring data for the McAfee ePO server is collected on an appliance.
Data collection interval in minutes	Time (in minutes) to elapse between data collections The time is set on a slider scale, ranging from . from 10 minutes to 6 hours.

Bypass ePO Requests rule set

The Bypass ePO Requests rule set is a library rule set for allowing requests from a McAfee ePO server to bypass filtering rules on an appliance.

Library rule set – Bypass ePO Requests
Criteria – *Command.Name equals "CONNECT"*
Cycles – Requests (and IM)

The rule set criteria specifies that the rule set applies when the SSL-secured communication between an ePO server and an appliance begins with a request from the server to connect to the appliance.

The rule set contains the following rule.

Skip subsequent rules for ePO requests

URL.Host equals "127.0.0.1" OR URL.Host equals "[::1]" –> Stop Cycle – Enable SSL Client Context<Default CA> – Enable SSL Scanner <Certificate verification without edh>

The rule uses the URL.Host property to identify the host of a requested URL, based on the IP address of the host.

If this address is 127.0.0.1, the host of the requested URL is the appliance. When the ePO server sends a request to connect to the appliance, it uses this address.

So if 127.0.0.1 is the requested address, the rule applies and stops all further processing in the request cycle. This way the CONNECT request is allowed to pass through.

The next step in this process is sending and verifying certificates. The rule includes an event to enable the sending of a client certificate that is issued by the default certificate authority.

You can modify the event settings to have the certificate issued by another authority.

When certificate verification has been completed, the SSL-secured communication can go ahead.

Event monitoring with SNMP

Events that occur on the appliance system can be monitored using SNMP.

When monitoring is performed under SNMP (Simple Network Management Protocol), an SNMP agent that runs on a host system sends messages about events that occur on this system to other host systems that are its clients.

The messages are known as *traps* under SNMP, while the host system that the SNMP agent runs on is known as *management station*. The host systems that receive messages from the agent are also management stations, in addition to this, they are known as *trap sinks*.

Particular users or user communities are given permission to view the information sent with the traps. System information is also provided in the Management Information Base (MIB), which uses a tree structure to present the information.

Configure the SNMP settings

You can configure the SNMP settings to enable the monitoring of system events on an appliance.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to configure SNMP monitoring on and click **SNMP**.
3. Configure the SNMP settings as needed.
4. Click **Save Changes**.

See also
SNMP settings on page 368

SNMP settings

The SNMP settings are settings for configuring the monitoring of system events under SNMP.

SNMP Port Settings

Settings for the ports of the SNMP agent on an appliance that listen to client requests

Table 18-26 SNMP Port Settings

Option	Definition
Listener address list	List of the ports that listen to client requests

The following table describes an entry in the listener address list.

Table 18-27 Listener address – List entry

Option	Definition
Protocol	Protocol used for the communication between a port and the clients it listens to • **UDP** — When selected, UDP is used for this communication • **TCP** — When selected, TCP is used for this communication
Listener address	IP address and port number of a listener port
Comment	Plain-text comment on a listener port

SNMP Protocol Options

Settings for SNMP protocol versions and user access to SNMP information

Table 18-28 SNMP Protocol Options

Option	Definition
SNMP v1	When selected, system events are monitored under version 1 of SNMP.
SNMP v2c	When selected, system events are monitored under version 2c of SNMP.
Communities for SNMPv1 and SNMPv2c access	List of user communities who are allowed access to SNMP information under versions 1 and 2c of SNMP
SNMP v3c	When selected, system events are monitored under version 3 of SNMP.
SNMP v3 users	List of users who are allowed access to SNMP information under version 3 of SNMP

The following tables describe the entries in the list of user communities and the list of SNMP v3 users.

Table 18-29 User communities – List entry

Option	Definition
Community string	String used for authenticating a user community to let it access SNMP information, for example, *public*
Allowed root OID	ID of the item on the MIB tree that is the beginning of the information with allowed access When * or no value is specified here, access to all information is allowed.
Allowed from	Host name or IP address of the host system that access to SNMP information is allowed from
Read-only access	When selected, only reading access to SNMP information is allowed.
Comment	Plain-text comment on a user community

Table 18-30 SNMP v3 users – List entry

Option	Definition
User name	Name of a user who is allowed access to SNMP information
Allowed root OID	ID of the item on the MIB tree that is the beginning of the informationwith allowed access When * or no value is specified here, access to all information is allowed.
Authentication	Authenticaton method used when SNMP information is accessed by a user
Encryption	Encryption method used when SNMP information is accessed by a user
Read-only access	When selected, only reading access to SNMP information is allowed.
Comment	Plain-text comment on a user

SNMP Trap Sinks

Settings for the host systems that receive SNMP messages

Table 18-31 SNMP Trap Sinks

Option	Definition
Trap sinks	List of the host systems, known as *trap sinks*, that receive messages about system events from the SNMP agent on an appliance

The following table describes an entry in the list of trap sinks.

Table 18-32 Trap sinks – List entry

Option	Definition
Host name or IP address	Host name or IP address of a host system that receivesSNMP messages, which are known as *traps*
Port	Port on a host system that listens for SNMP messages
Community string	String used for authenticating a user community to let it access SNMP information, for example, *public*
Send SNMP v2c traps	When selected, messages can be sent under version v2c of the SNMP protocol.
Comment	Plain-text comment on a host system that receives SNMP messages

19 Troubleshooting

Several methods and tools are available for troubleshooting problems on an appliance.

Contents

Troubleshooting methods

When problems arise on an appliance, you can use different methods to solve them.

Record and inspect data in files

You can record data on appliance behavior in files and inspect them. The following types of files can be created for this purpose:

- **Log files** — Log events and functions, such as access to an appliance or updates of files
- **Rule tracing files** — Record the processing of rules
- **Feedback files** — Backtrace processes after the failure of a function
- **Core files** — Record memory content after the failure of a function has caused an appliance to terminate operation
- **Connection tracing files** — Record activities on connections between an appliance and other network components
- **Packet tracing files** — Record network activities of an appliance

Use network tools

You might need to test whether connections from an appliance to other network components still work. Several tools are available for this purpose, including *ping*, *nslookup*, *ipneigh*, and others.

Restore a configuration

When other troubleshooting methods do not work, it might be necessary to remove a faulty appliance configuration and replace it with a backup.

Having a backup available can also help in other situations, for example, when you want to discard changes applied to an existing configuration.

Options are provided for creating backups and using them to restore configurations.

Create a feedback file

You can create a feedback file to backtrace processes after the failure of a function.

Task

1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to backtrace processes on and click **Feedback**.
3. Select or deselect **Pause running McAfee Web Gateway to create a backtrace** as needed.

   ℹ We recommend that you select the checkbox.

4. Click **Create Feedback File**.

   A feedback file is created and appears with its name, size, and date in the list under **Feedback file**.

Using the items on the toolbar, you can perform several file-related activities, such as view or download a file.

Enable the creation of core files

You can enable the creation of core files to record memory content after the failure of a function has caused an appliance to terminate operation.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to record memory content on and click **Troubleshooting**.
3. In the **Troubleshooting** section, select **Enable core file creation**.
4. Click **Save Changes**.

   Core files are now created whenever the appliance terminates due to the failure of a particular function.

You can view the core files, after selecting the appliance under the **Troubleshooting** top-level menu and clicking **Core Files**. The files are then displayed in a list.

Using the items on the toolbar, you can perform several file-related activities, such as view or download a file.

Enable the creation of connection tracing files

You can enable the creation of trace files to record activities occurring on connections between an appliance and other network components.

Task

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to record connection activities on and click **Troubleshooting**.
3. In the **Troubleshooting** section, select **Enable connection tracing**.
4. [Optional] To trace only activities on a connection to a particular client of the appliance, select **Restrict tracing to only one IP** and type the IP address of the client in the **Client IP** field.
5. Click **Save Changes**.

   Connection tracing files are now created.

You can view the connection tracing files, after selecting the appliance under the **Troubleshooting** top-level menu and clicking **Connection Tracing**. The files are then displayed in a list.

Using the items on the toolbar, you can perform several file-related activities, such as view or download a file.

Create a packet tracing file

You can create a packet tracing file to record the network activities of an appliance.

Task

1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to record network activities on and click **Packet tracing**.
3. In the **Command line parameters** field, type parameters for the packet tracing as needed.
4. Click **tcpdump start**.

   A packet tracing file is generated and appears with its name, size, and date in the list under **Results (dump)**.

   To stop the ongoing generation of a packet tracing file, click **tcpdump stop**.

Using the items on the toolbar of the list, you can perform several file-related activities, such as view or download a file.

Work with network tools

You can work with several network tools to troubleshoot problems on an appliance.

Task

1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to use a network tool on and click **Network Tools**.
3. In the **Command line parameters** field, type the parameters for a command that is provided by a particular network tool.

   For example, type the name of a host you want to connect to using the *ping* command.
4. Click the button for one of the following network tools:
   - **ping**
   - **ping6**
   - **nslookup**
   - **traceroute**
   - **traceroute6**
   - **ipneigh**
   - **service restart**
   - **ntp**

   The corresponding command is executed and the output displayed in the **Results** field.

   Output could, for example, look like this:

   ```
   Ping: Unknown host testhost
   ```

Back up and restore an appliance configuration

You can store an appliance configuration in a backup file and use this file to restore the configuration.

When restoring a configuration, you can choose to restore the complete configuration or only the data configured under the **Policy** top-level menu, which includes data on rules, lists, and settings.

Task

1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to back up or restore a configuration for and click **Backup/Restore**.

3 Under **Backup policy, configuration, and accounts**, proceed as follows:

- To back up a configuration, click **Backup to File**.

  Your local file manager opens to let you select a file for storing a configuration backup.

- To restore:

  - The complete configuration

    Deselect **Only restore policy**, then click **Restore From File**.

  - Only rules, lists, and settings

    Make sure **Only restore policy** is selected, then click **Restore From File**.

  Confirm the message that you will be logged off after restoring.

  Your local file manager opens to let you select a backup file for restoring the configuration.

A Configuration lists

The following lists describe items you can use to configure web security rules.

Contents

List of actions

The following table provides a list of the actions you can use in rules.

The actions are listed in alphabetical order.

Table A-1 List of actions

Action	Description
Authenticate	Stops processing the rules in the current cycle. Sends an authentication request to the client of the user who requested access to a web object. Continues processing with the next cycle.
Block	Blocks access to a requested web object. Stops processing rules. Continues when the next request is received on the appliance.
Continue	Continues processing with the next rule.
Redirect	Redirects a client that requested access to a web object to another object.
Remove	Removes a requested web object. Stops processing the rules in the current cycle. Continues processing with the next cycle.
Stop Cycle	Stops processing the rules in the current cycle. Does not block access to a requested web object. Continues processing with the next cycle.
Stop Rule Set	Stops processing the rules of the current rule set. Continues processing with the next rule set.

List of error IDs

The following table provides a list of the error IDs you can use in rules.

The error IDs are grouped in numerical ranges as follows.

10000–10049	Incorrect usage of properties or events
10050–10099	Errors of the rule processing module
10100–10199	General errors
11000–11999	License Manager errors
12000–12999	Errors related to the appliance system
13000–13999	Persistent Database (PDStore) errors
14000–14999	Virus and malware filtering errors
15000–15999	URL filtering errors
16000–16999	ICAP client errors
20000–21000	Proxy module errors
25000–25999	External lists errors
26000–26999	Data loss prevention (DLP) errors

Table A-2 List of error IDs

Error ID	Error name	Error message
10000	WrongPropParams	$onPosition$: Wrong parameters or types for property $propName$.
10001	UnknownProperty	$onPosition$: Error in rule ‘$ruleName$’: Property dispatcher does not know property $propName$.
10002	NoPropParam	$onPosition$: No parameter for property $propName$ given.
10003	WrongThirdPropParam	$onPosition$: Wrong type of third parameter for property $propName$.
10004	InvalidPropertyParameter	$onPosition$: Parameters for property $propName$ are invalid, reason: $reason$.
10005	InvalidPropertyParameter2	Parameters are invalid. Reason: $reason$.
10005	UnknownProperty2	$onPosition$: Unknown property $propName$.
10007	UnknownFunc	$onPosition$: Unknown function $funcName$. Details: $reason$.
10050	WrongOperator	$onPosition$: Error in rule '$ruleName$': wrong operator '$operator$' used on left hand side type $typeLeft$ and right hand side type $typeRight$.
10051	WrongOperatorNoNames	$onPosition$: $action$ failed. Type of $property$ is $typeName$, but it has to be $formatType$.
10052	FormatError	$onPosition$: User-defined property '$propName$' could not be found. Reason: it was not yet set (not initialized).
10053	UserDefinedPropertyNotFound	$onPosition$: User-defined property '$propName$' could not be found. Reason: it was not yet set (not initialized).
10054	PropertyNotFound	$onPosition$: Property '$propName$' could not be found. Reason: it was not yet set (not initialized).
10055	NeedMoreDataOnLastCall	On computing property '$propName$' the filter returned 'NeedMoreData' though there is no more data.

Table A-2 List of error IDs *(continued)*

Error ID	Error name	Error message
10056	WrongPropState	$onPosition$: State of Property $propName$ is $propState $.
10057	ZombieRuleElemIsExecuted	$rule$ (name: '$name$', id: '$id$') could not be executed because it is a zombie. Reason: '$reason$'.
10058	SetPropertyFailed	$onPosition$: Error in Rule '$ruleName$': Event could not be evaluated. Reason: $reason$.
10059	EventError	$onPosition$: Error while $operation$ the $objName$. Reason: $reason$.
10100	ErrorDuringOperation	$onPosition$: Error while $operation$ the $objName$. Reason: $reason$.
10101	InitializeFailed	$onPosition$: Could not initialize/create $objName$. Reason:$reason$.
11000	NoLicense	The requested functionality '$func$' is not covered by your license.
12000	CannotOpenPipe	Cannot open pipe.
12001	CannotOpenFile	Cannot open file '$name$' in mode '$mode$' with errno '$errno$'.
13000	NoUser	No user available.
14000	AVError	Error in AntivirusFilter: $reason$.
14001	AVScanFailedFull	Cannot call McAfee Gateway Anti-Malware engine. All connections in use.
15000	TSDatabaseExpired	Global Threat Intelligence system database expired error: Database is expired. '$desc$'.
15001	TSInvalidURL	The URL '$url$' is invalid. In function $func$.
15002	TSBinaryNotProperlyLoaded	Binary could not be loaded from '$path$'. In function $func $.
15003	TSCommon	Global Threat Intelligence system error (code: $errorCode $). In function $func$.
15004	TSBinaryDoesNotExist	Global Threat Intelligence system library is not yet available. In function $func$.
15005	TSDatabaseNotProperlyLoaded	Database was not properly loaded. In function $func$.
15006	TSNoMem	Global Threat Intelligence system is out of memory. In function $func$.
15007	TSInsufficientSpace	Insufficient space in buffer for Global Threat Intelligence system. In function $func$.
15008	TSNetLookup	Global Threat Intelligence system net error (code: TS_NET_ERROR). In function $func$.
15009	TSCommonNetLookup	Global Threat Intelligence system net error (code: $errorCode$). In function $func$.
15010	TSPipe	Cannot open Global Threat Intelligence system pipe. In function $func$.
16000	NoICAPServerAvailable	No ICAP server available from list: $list$ dyx.
20000	CheckLongRunningConnection	Check for long running connections.
25000	Unknown error happened	An uncategorized error was encountered by the External Lists module.

Table A-2 List of error IDs *(continued)*

Error ID	Error name	Error message
25001	Error during data fetch	An uncategorized error was encountered by the External Lists module during the data fetch.
25002	Error during data conversion	An error occurred while external list data was converted.
25003	Too much data	The configured limit for the number of list entries that can be retrieved from an external source has been exceeded.
25004	Timeout during data fetch	The configured timeout for retrieving external list data has expired.
25005	Data access denied	The rights required for accessing a source of external list data have not been granted to the appliance.
25006	No such resource	A source of external list data, for example, a file or web server, could not be found.
26001	DLP engine not loaded	The DLP engine could not be loaded.

List of events

The following table provides a list of the events you can use in rules.

The events are listed in alphabetical order.

Table A-3 List of events

Name	Description	Parameters
Authentication.AddMethod	Adds an authentication method.	1 String: Name of an authentication method 2 String: Value for an authentication method 3 Boolean: If true, an existing method is overwritten.
Authentication.ClearCache	Clears the cache.	
Authentication.ClearMethodList	Clears the authentication methods list.	
Authentication.ClearNTMLCache	Clears the NTML cache.	
BlockingSession.Activate	Activates a blocking session.	
Body.Insert	Inserts a string into body of a message.	1 Number: Byte position where insertion begins 2 String: Pattern a. string embedded in double quotes (" ...", can also contain hex values preceded by \) *or:* b. sequence of hex values

Table A-3 List of events *(continued)*

Name	Description	Parameters
Body.Remove	Removes a number of bytes from a body.	1 Number: Byte position where the removal begins 2 Number: Number of bytes to remove
Body.Replace	Replaces a portion of a body with a string.	1 Number: Byte position where replacement begins 2 String: Pattern a. string embedded in double quotes (" ...", can also contain hex values preceded by \\) *or:* b. sequence of hex values
Connection.Mark	Sets a connection mark.	Number: Number of a connection
Email.Send	Sends an email.	1 String: Recipient 2 String: Subject 3 String: Body
Enable Cache	Enables the web cache.	
Enable CompositeOpener	Enables the composite opener.	
Enable Data Trickling	Enables data trickling.	
Enable HTML Opener	Enables the HTML opener.	
Enable Next Hop Proxy	Enables use of next-hop proxies.	
Enable Progress Page	Enables display of a progress page.	
Enable RuleEngine Tracing	Enables tracing of the rule processing module.	
Enable SSL Client Context with CA	Enables sending of client certificates issued by a certificate authority.	
Enable SSL Client Context without CA	Enables sending of client certificates not issued by a certificate authority.	
Enable SSL Scanner	Enables module for SSL scanning.	
Enable SafeSearchEnforcer	Enables the SafeSearchEnforcer.	
Enable Workaround	Enables a workaround.	

Table A-3 List of events *(continued)*

Name	Description	Parameters
FileSystemLogging.WriteDebugEntry	Writes a debugging entry.	1 String: Debugging entry 2 Boolean: If true, entry is written to stdout.
FileSystemLogging.WriteLogEntry	Writes an entry into a log.	String: Log entry
HTMLElement.InsertAttribute	Inserts an attribute into an HTML element.	1 String: Attribute name 2 String: Attribute value
HTMLElement.RemoveAttribute	Removes an attribute from an HTML element.	String: Attribute name
HTMLElement.SetAttributeValue	Sets an attribute to a value.	1 String: Attribute name 2 String: Value to set attribute to
Header.Add	Adds a header to a request or response.	1 String: Header name 2 String: Header value
Header.AddMultiple	Adds a header with a list of values to a request or response.	1 String: Header name 2 List of string: List of header values
Header.Block.Add	Adds a block header to a request or response.	1 String: Header name 2 String: Header value
Header.Block.AddMultiple	Adds a block header with a list of values to a request or response.	1 String: Header name 2 List of string: List of header values
Header.Block.RemoveAll	Removes all block headers with a given name from a request or response.	String: Header name
Header.ICAP.Response.Add	Adds a header to an ICAP response.	1 String: Header name 2 String: Header value
Header.ICAP.Response.AddMultiple	Adds a header with a list of values to an ICAP response.	1 String: Header name 2 List of string: List of header values
Header.ICAP.Response.RemoveAll	Removes all headers with a given name from an ICAP response.	String: Header name
Header.RemoveAll	Removes all headers with a given name from a request or response.	String: Header name
ICAP.AddRequestInformation	Adds information to an ICAP request.	1 String: Name of the request 2 String: Added information

Table A-3 List of events *(continued)*

Name	Description	Parameters
MediaType.Header.FixContentType	Replaces a media type header with an appropriate header when it is found after inspection of the media body that	
Notice	Writes an entry with notice level into syslog.	String: Log entry
PDStorage.AddGlobalData.Bool	Adds global variable of type Boolean.	1 String: Variable key 2 Boolean: Variable value
PDStorage.AddGlobalData.Category	Adds global variable of type Category.	1 String: Variable key 2 Category: Variable value
PDStorage.AddGlobalData.Dimension	Adds global variable of type Dimension.	1 String: Variable key 2 Dimension: Variable value
PDStorage. AddGlobalData.Hex	Adds global variable of type Hex.	1 String: Variable key 2 Hex: Variable value
PDStorage. AddGlobalData.IP	Adds global variable of type IP.	1 String: Variable key 2 IP: Variable value
PDStorage.AddGlobalData.IPRange	Adds global variable of type IPRange.	1 String: Variable key 2 IPRange: Variable value
PDStorage.AddGlobalData.List.Category	Adds global variable of type List of Category.	1 String: Variable key 2 List of Category: Variable value
PDStorage. AddGlobalData.List. Dimension	Adds global variable of type List of Dimension.	1 String: Variable key 2 List of Dimension: Variable value
PDStorage.AddGlobalData.List.Hex	Adds global variable of type List of Hex.	1 String: Variable key 2 List of Hex: Variable value
PDStorage. AddGlobalData.List.IP	Adds global variable of type List of IP.	1 String: Variable key 2 List of IP: Variable value
PDStorage. AddGlobalData.List.IPRange	Adds global variable of type List of IPRange.	1 String: Variable key 2 List of IPRange: Variable value
PDStorage.AddGlobalData.List.MediaType	Adds global variable of type List of MediaType.	1 String: Variable key 2 List of MediaType: Variable value

Table A-3 List of events *(continued)*

Name	Description	Parameters
PDStorage. AddGlobalData.List. Number	Adds global variable of type List of Number.	1 String: Variable key 2 List of Number: Variable value
PDStorage. AddGlobalData.List. String	Adds global variable of type List of String.	1 String: Variable key 2 List of String: Variable value
PDStorage. AddGlobalData.List. Wildcard	Adds global variable of type List of Wildcard Expression.	1 String: Variable key 2 List of Wildcard Expression: Variable value
PDStorage. AddGlobalData. MediaType	Adds global variable of type MediaType.	1 String: Variable key 2 MediaType: Variable value
PDStorage. AddGlobalData.Number	Adds global variable of type Number.	1 String: Variable key 2 Number: Variable value
PDStorage. AddGlobalData.String	Adds global variable of type String.	1 String: Variable key 2 String: Variable value
PDStorage. AddGlobalData. Wildcard	Adds global variable of type Wildcard Expression.	1 String: Variable key 2 Wildcard Expression: Variable value
PDStorage. AddUserData.Bool	Adds user variable of type Boolean.	1 String: Variable key 2 Boolean: Variable value
PDStorage. AddUserData.Category	Adds user variable of type Category.	1 String: Variable key 2 Category: Variable value
PDStorage. AddUserData. Dimension	Adds user variable of type Dimension.	1 String: Variable key 2 Dimension: Variable value
PDStorage. AddUserlData.Hex	Adds user variable of type Hex.	1 String: Variable key 2 Hex: Variable value
PDStorage. AddUserData.IP	Adds user variable of type IP.	1 String: Variable key 2 IP: Variable value
PDStorage. AddUserData.IPRange	Adds user variable of type IPRange.	1 String: Variable key 2 IPRange: Variable value
PDStorage. AddUserData.List. Category	Adds user variable of type List of Category.	1 String: Variable key 2 List of Category: Variable value

Table A-3 List of events *(continued)*

Name	Description	Parameters
PDStorage. AddUserData.List. Dimension	Adds user variable of type List of Dimension.	1 String: Variable key 2 List of Dimension: Variable value
PDStorage. AddUserData.List.Hex	Adds user variable of type List of Hex.	1 String: Variable key 2 List of Hex: Variable value
PDStorage. AddUserData.List.IP	Adds user variable of type List of IP.	1 String: Variable key 2 List of IP: Variable value
PDStorage.AddUserData.List.IPRange	Adds user variable of type List of IPRange.	1 String: Variable key 2 List of IPRange: Variable value
PDStorage.AddUserData.List.MediaType	Adds user variable of type List of MediaType.	1 String: Variable key 2 List of MediaType: Variable value
PDStorage.AddUserData.List.Number	Adds user variable of type List of Number.	1 String: Variable key 2 List of Number: Variable value
PDStorage.AddUserData.List.String	Adds user variable of type List of String.	1 String: Variable key 2 List of String: Variable value
PDStorage.AddUserData.List.Wildcard	Adds user variable of type List of Wildcard Expression.	1 String: Variable key 2 List of Wildcard Expression: Variable value
PDStorage.AddUserData.MediaType	Adds user variable of type MediaType.	1 String: Variable key 2 MediaType: Variable value
PDStorage.AddUserData.Number	Adds user variable of type Number.	1 String: Variable key 2 Number: Variable value
PDStorage.AddUserData.String	Adds user variable of type String.	1 String: Variable key 2 String: Variable value
PDStorage.AddUserData.Wildcard	Adds user variable of type Wildcard Expression.	1 String: Variable key 2 Wildcard Expression: Variable value
PDStorage.Cleanup	Cleans up persistently stored data.	
PDStorage. DeleteAllUserData	Deletes all permanently stored user data.	

Table A-3 List of events *(continued)*

Name	Description	Parameters
PDStorage.DeleteGlobalData	Deletes all permanently stored global variables of a given type.	String: Variable key
PDStorage.DeleteUserData	Deletes all permanently stored user variables of a given type.	String: Variable key
SNMP.Send.Trap.Application	Sends an SNMP trap message with application information.	
SNMP.Send.Trap.System	Sends an SNMP trap message with system information.	
SNMP.Send.Trap.User	Sends an SNMP trap message with user information.	1 Number: User ID 2 String: Message body
SNMP.Send.Trap.UserHost	Sends an SNMP trap message with information on the host of a user.	1 Number: User ID 2 String: Message body 3 IP: IP address of the host
Statistics.Counter.Increment	Increments a counter.	1 String: Counter name 2 Number: Increment value
Statistics.Counter.Reset	Resets a counter.	String: Counter name
Stopwatch.Reset	Sets an internal watch that measures processingtime for rule sets to zero.	String: Rule set name
Stopwatch.Start	Starts an internal watch that measures processing time for rule sets.	String: Rule set name
Stopwatch.Stop	Stops an internal watch that measures processing time for rule sets.	String: Rule set name
Syslog	Writes an entry into syslog.	1 Number: Log level 0 – Emergency 1 – Alert 2 – Critical 3 – Error 4 – Warning 5 – Notice 6 – Info 7 – Debugging 2 String: Log entry

List of incident IDs

The following table provides a list of the incident IDs you can use in rules.

The incident IDs are grouped in numerical ranges as follows.

1–199	Incidents related to the appliance system
200–299	Core subsystem incidents
300–399	Update module incidents
500–599	Log File Manager incidents
600–699	*sysconfd* daemon incidents
700–799	Proxy module incidents
800–899	Virus and malware filtering incidents
900–999	Authentication incidents
1000–1099	URL filtering incidents
1600–1699	SSL certificate incidents
1900–1999	Data loss prevention (DLP) incidents
3000–3200	Central Management incidents

Table A-4 List of incident IDs

Incident ID	Description	Origin number and name	Severity
5	A rule that uses an incident property has been executed.	1 System	7
20	RAID monitoring reports critical status or failure of one or more hard disks.	1 Health monitor	4 (or 3 for hard-disk failure)
21	S.M.A.R.T health check reports an error on a HDD hard disk.	1 Health monitor	4
22	File system usage exceeds a configured limit.	1 Health monitor	4
23	Memory usage exceeds a configured limit.	1 Health monitor	4
24	System load exceeds a configured limit.	1 Health monitor	4
200	The license expiration date has been checked.	2 Core	6
201	The appliance has successfully completed all FIPS 140-2 self-tests.	2 Core	6
301	Download of update files was stopped because there is not enough disk space.	3 Updater	3
302	Download of product x failed for node y in central management.	3 Updater	3
303	The update module reports that update of product x failed on node y in Central Management.	3 Updater	3
304	The update module received a report from an update server that status of product x is up to date.	3 Updater	3
305	The update module could not connect to an update server.	3 Updater	3
501	The Log File Manager failed to push log files.	5 Log File Manager	3
601	Data packages involved in a yum update require an restart of the appliance to become effective.	6 mwg-update	4

Table A-4 List of incident IDs *(continued)*

Incident ID	Description	Origin number and name	Severity
666	A FIPS 140-2 self-test failed on node y in central management. The node is running in non-FIPS mode.	1 FIPS	0
700	The number of concurrent connections exceeds a configured overload limit. The appliance enters overload state. Requests sent to the appliance are accepted with delay.	2 Proxy	2
701	The appliance is in overload state for more than 30 seconds. Requests sent to the appliance are accepted with delay.	2 Proxy	2
702	The appliance has left overload state. Requests sent to the appliance are again accepted without delay.	2 Proxy	4
703	The number of concurrent connections exceeds a configured high-load limit. The appliance enters high-load state. Requests sent to the appliance are accepted with a delay.	2 Proxy	4
704	The appliance is in high-load state for more than 30 seconds. Requests sent to the appliance are accepted with a delay.	2 Proxy	4
705	The number of concurrent connections has dropped below 85 % of a configured high-load limit. The appliance is still in high-load state. Requests sent to the appliance are accepted with a delay.	2 Proxy	6
710	A next-hop proxy server is down and will not be available for n seconds.	2 Proxy	4
711	The appliance cannot connect to a next-hop proxy server.	2 Proxy	4
712	A next-hop proxy server has moved back from error state to normal operation.	2 Proxy	6
720	The listener on IP address x, port y could not be opened.	2 Proxy	2
730	A changed proxy mode configuration requires restart of the appliance.	2 Proxy	2
850	An update of the Anti-Malware module was completed successfully.	2 Anti-Malware Filter	6
851	An update of the Anti-Malware module failed.	2 Anti-Malware Filter	3
852	Download or verification of update files for the Anti-Malware module failed.	2 Anti-Malware Filter	3
853	The Anti-Malware module version is up to date.	2 Anti-Malware Filter	6
901	The appliance is connected to n servers for NTML authentication in Windows domain x.	2 Core	6
902	The appliance cannot connect to n servers for NTML authentication in Windows domain x.	2 Core	4
903	The appliance cannot contact Windows domain x for NTLM authentication.	2 Core	3
910	The appliance is connected to the LDAP server with configuration ID n.	2 Core	6

Table A-4 List of incident IDs *(continued)*

Incident ID	Description	Origin number and name	Severity
912	The appliance is disconnected from the LDAP server with configuration ID n.	2 Core	4
913	The appliance cannot connect to any LDAP server with configuration ID n.	2 Core	3
920	A response has been received on the appliance from RADIUS server x after attempting to start communication with this server to retrieve user information for authentication purposes.	2 Core	6
921	A response has again been received on the appliance from RADIUS server x after communication with this server had been interrupted.	2 Core	6
923	An authentication request sent from the appliance to RADIUS server x has led to a timeout.	2 Core	3
931	The appliance is connected to NTLM-Agent server x.	2 Core	6
932	The appliance is disconnected from NTLM-Agent server x.	2 Core	3
933	The appliance cannot connect to NTLM-Agent server x.	2 Core	3
1050	An update of the URL Filter module was completed successfully.	2 URL Filter	6
1051	An update of the URL Filter module failed.	2 URL Filter	3
1052	Download or verification of update files for the URL Filter module failed.	2 URL Filter	3
1053	URL Filter module status is up to date.	2 URL Filter	6
1650	An updated Certificate Revocation List (CRL) was downloaded and loaded successfully on the appliance.	2 Certificate Chain Filter	6
1651	An updated Certificate Revocation List (CRL) was downloaded to the appliance, but could not be loaded there.	2 Certificate Chain Filter	4
1652	An updated Certificate Revocation List (CRL) could not not be downloaded to the appliance.	2 Certificate Chain Filter	
1653	All Certificate Revocation Lists (CRLs) used by the SSL Scanner module have up-to-date status.	2 Certificate Chain Filter	6
1950	An update of the DLP module was completed successfully.	2 DLP Engine	6
1951	An update of the DLP module failed.	2 DLP Engine	3
1952	Download or verification of the update files for the DLP module failed.	2 DLP Engine	3
1953	DLP module status is up to date.	2 DLP Engine	6
3000	At least one node in a Central Management configuration is not in synchronized state (regarding storage and configuration). The number of unsynchronized nodes changes. This incident is only recorded on the root node.	3 Central Management	3

Table A-4 List of incident IDs *(continued)*

Incident ID	Description	Origin number and name	Severity
3001	After incident 3000 has occurred, all nodes in a Central Management configuration are in synchronized state again (regarding storage and configuration).	3 Central Management	6
3004	At least one node in a Central Management configuration did not respond properly after shared data was sent out. The number of not properly responding nodes changes. This incident is only recorded on the root node and only if the shared data was intended to go to all nodes.	3 Central Management	3
3005	After incident 3004 has occurred, all nodes in a Central Management configuration have properly responded to the sending of shared data to them.	3 Central Management	6

List of properties

The following table provides a list of the properties you can use in rules.

The properties are listed in alphabetical order. However, the listing takes into consideration the parts of the property names, which are separated by periods.

This means that, for example, *SSL.Server.Certificate.DaysExpired* is listed before *SSL.Server.CertificateChain.ContainsExpiredCA.*

Table A-5 List of properties – A

Name	Type	Description	Parameters
Antimalware.Infected	Boolean	If true, a web object has been found to be infected.	
Antimalware.Proactive.Probability	Number	Probability that a web object is malware The probability is a percentage, specified by a number from 1 to 100.	
Antimalware.VirusNames	List of String	List with names of the viruses that a web object has been found to be infected with	
Application.IsHighRisk	Boolean	If true, access to an application is considered to be a high risk for web security.	
Application.IsMediumRisk	Boolean	If true, access to an application is considered to be a medium risk for web security.	
Application.IsMinimalRisk	Boolean	If true, it has not been verified whether access to an application is a risk for web security.	
Application.IsUnverified	Boolean	If true, access to an application is considered to be a high risk for web security.	
Application.Name	Applcontrol	Name of an application	
Application.Reputation	Number	Reputation score for an application	

Table A-5 List of properties – A *(continued)*

Name	Type	Description	Parameters
Application.ToString	String	Name of an application converted into a string	Applcontrol: Application name to convert
Authentication.Authenticate	Boolean	If true, the authentication engine has been called to apply the configured method, for example, NTLM, to the credentials of a user and the user has successfully been authenticated. Values have also been set for the *Authentication.IsAuthenticated* and *Authentication.UserName* properties. If false, it was not possible to apply the configured authentication method successfully, for example, because no credentials or incorrect credentials were submitted.	
Authentication. CacheRemainingTime	Number	Time (in seconds) that remains until authentication credentials are cleared from the cache	
Authentication.Failed	Boolean	If true, credentials were provided by a user, but authentication has failed.	
Authentication.FailureReason	Number	Number identifying the reason why authentication has failed for a user	
Authentication.GetUserGroups	List of String	List of user groups that the authentication process is applied to	
Authentication.IsAuthenticated	Boolean	If true, a user has been successfully authenticated.	
Authentication. IsLandingOnServer	Boolean	If true, cookie authentication has been applied for a user.	
Authentication.IsServerRequest	Boolean	If true, authentication has been requested for a user under the Authentication Server method.	
Authentication.Method	String	Method used for authenticating a user, for example, LDAP	
Authentication.RawCredentials	String	Credentials of a user in the format originally received on the appliance from a client or other instances of the network Using this property for rule configuration will speed up processing because it saves the time used for converting user credentials to a human readable format, as it is done for the simple *Authentication.UserName* property.	

Table A-5 List of properties – A *(continued)*

Name	Type	Description	Parameters
Authentication.RawUserName	String	Name of a user in the format originally received on the appliance from a client or other instances of the network Using this property for rule configuration will speed up processing because it saves the time used for converting the user name to a human readable format, as it is done for the simple *Authentication.UserName* property.	
Authentication.Realm	String	Authentication realm, for example, a Windows domain	
Authentication.UserGroups	List of string	List of user groups that the authentication process is applied to	
Authentication.UserName	String	Name of a user that the authentication process is applied to	

Table A-6 List of properties – B

Name	Type	Description	Parameters
Block.ID	Number	ID of an action that blocked a request	
Block.Reason	String	Name of the reason for an action that blocked a request	
BlockingSession.IsBlocked	Boolean	If true, a blocking session has been activated for a user.	
BlockingSession. RemainingSession	Number	Remaining time of a blocking session (in minutes)	
BlockingSession. SessionLength	Number	Time length of a blocking session (in minutes)	
Body.ChangeHeaderMime	Boolean	If true, the header sent in MIME format with the body of a web object has been changed.	
Body.ClassID	String	ID for a class of web objects	
Body.Equals	Boolean	If true, the body of a web object matches the pattern specified by the property parameters.	1 Number: Position of byte where pattern begins 2 String: Pattern a. String embedded in double quotes (" ...", can also contain hex values preceded by \) *or:* b. Sequence of hex values
Body.FileName	String	Name of a file that is embedded in the body of a web object, for example, an archived file	

Table A-6 List of properties – B *(continued)*

Name	Type	Description	Parameters
Body.FullFileName	String	Name of a file that is embedded in the body of a web object, including also the names of the embedding entities, such as documents or archives Name parts are separated by the | (pipe) symbol, for example, *test.zip|test.doc*.	
Body.HasMimeHeader	Boolean	If true, the body of an extracted multi-part object sent in MIME format has a specified header.	String: Header name
Body. HasMimeHeaderParameter	Boolean	If true, the body of an extracted multi-part object sent in MIME format has a specified header parameter.	1 String: Header name 2 String: Header parameter name
Body.IsAboveSizeLimit	Boolean	If true, the body of a web object is above a size limit.	
Body.IsCompleteWithTimeout	Boolean	If true, the body of a web object has been completely sent to the appliance before the time (in milliseconds) specified by the property parameter has elapsed.	Number: Time allowed to send object completely (in milliseconds)
Body.IsCorrupted Object	Boolean	If true, an archive contained in the body of a web object is corrupted.	
Body.IsEncrypted Object	Boolean	If true, an archive contained in the body of a web object is encrypted.	
Body.IsMultiPartObject	Boolean	If true, an archive contained in the body of a web object is complex, including multiple parts.	
Body.IsSupportedByOpener	Boolean	If true, an opener device is available on the appliance for the body of a web object that is composite, for example,the body of an archive.	
Body. MimeHeaderParameterlValue	String	Value of a header parameter in the body of a web object sent in MIME format	1 String: Header name 2 String: Header parameter value
Body.MimeHeaderValue	String	Value of a header in the body of a web object sent in MIME format	String: Header value
Body.Modified	Boolean	If true, an appliance module has modified the body of a web object.	

Table A-6 List of properties – B *(continued)*

Name	Type	Description	Parameters
Body.NestedArchive Level	Number	Current level of an archive part in an archive	
Body.NotEquals	Boolean	If false, the body of a web object matches the pattern specified by the property parameters.	1 Number: Position of byte where pattern begins 2 String: Pattern a. String embedded in double quotes (" ...", can also contain hex values preceded by \) *or:* b. Sequence of hex values
Body.NumberOfChildren	Number	Number of objects embedded in the body of a web object	
Body.PositionOfPattern	Number	Position of the byte where the search for a pattern in the body of a web object begins Returns -1 if the pattern is not found.	1 String: Pattern to search for a. String embedded in double quotes (" ...", can also contain hex values preceded by \) *or:* b. Sequence of hex values 2 Number: Position of byte where search for pattern begins 3 Number: Search length (in bytes, 0 means search from offset to end of object)
Body.Size	Number	Size of the body of a web object (in bytes)	
Body.Text	String	Text in the body of a web object	
Body.ToNumber	Number	Part of the body of a web object converted into a number (maximum 8 bytes beginning at a specified position) The big-endian or little-endian format can be used for the conversion.	1 Number: Position of byte where converted part begins 2 Number: Length of converted part (in bytes, maximum 8) 0 for the first parameter and the respective value of the *Body.Size* property for the second means the whole body is converted. 3 Boolean: If true, little-endian format is used for conversion,otherwise big-endian

Table A-6 List of properties – B *(continued)*

Name	Type	Description	Parameters
Body.ToString	String	Part of the body of a web object converted into a string	1 Number: Position of byte where converted part begins 2 Number: Length of converted part (in bytes) 0 for the first parameter and the respective value of the *Body.Size* property for the second means the whole body is converted.
Body.UncompressedSize	Number	Size of the body of an archived web object (in bytes) after having been extracted from the archive	
BooleanToString	String	Boolean value converted into a string	Boolean: Boolean value to convert
BytesFromClient	Number	Number of bytes received in a request from a client	
BytesFromServer	Number	Number of bytes received in a response from a web server	
BytesToClient	Number	Number of bytes in a web server response that is forwarded to a client	
BytesToServer	Number	Number of bytes in a client request that is forwarded to a web server	

Table A-7 List of properties – C

Name	Type	Description	Parameters
Cache.IsCacheable	Boolean	If true, an object sent in response from a web server can be stored in the web cache.	
Cache.IsFresh	Boolean	If true, an object stored in the web cache has either been downloaded from the web or has been verified.	

Table A-7 List of properties – C *(continued)*

Name	Type	Description	Parameters
Cache.Status	String	Cache status for a web object Values: • *TCP_HIT* – A web object was requested by a user and found in the cache. • *TCP_MISS* – A web object was requested by a user and not found in the cache. • *TCP_MISS_RELOAD* – A web object was requested by a user, but was not taken from the cache because the user required it to be fetched directly from the web server in question by clicking the **Refresh** button. The object was then entered into the cache again. • *TCP_MISS_VERIFY* – A web object was requested by a user and existed in the cache, but verification information from the web server in question showed it was outdated. An updated version of the object was received from the server and entered into the cache.	
Category.ToShortString	String	URL category converted into a string that is the category abbreviation	Category: Category to convert
Category.ToString	String	URL category converted into a string	Category: Category to convert
Client.IM.Login	String	ID used by a client to log on to the appliance under an instant messaging protocol	
Client.IM.ScreenName	String	Screen name of of a client communicating with the appliance under an instant messaging protocol	
Client.IP	IP	IP address of a client	
Client.NumberOfConnections	Number	Number of connections from a client to the appliance that are open at the same time	
Command.Categories	List of String	List of categories that a command belongs to, for example, to the FTP command category	
Command.Name	String	Name of a command	
Command.Parameter	String	Parameter of a command	
Connection.Aborted	Boolean	If true, communication on a connection has finally failed and the connection is closed.	
Connection.IP	IP	IP address used on a connection	
Connection.Protocol	String	Protocol used for communication on a connection, for example, HTTP	

Table A-7 List of properties – C *(continued)*

Name	Type	Description	Parameters
Connection.Protocol.IsIM	Boolean	If true, communication on a connection uses an instant messaging protocol .	
Connection.RunTime	Number	Time (in seconds) a connection has been running since it was opened until the current second	
Connection.SSL. TransparentCNHandling	Boolean	If true, communication on a connection is SSL-secured and runs in transparent mode.	
Cycle.LastCall	Boolean	If true, processing of data is complete for a cycle.	
Cycle.Name	String	Name of a processing cycle	
Cycle.TopName	String	Name of a cycle (Requests or Responses) that is processed before a web object is processed in the Embedded Objects cycle	

Table A-8 List of properties – D

Name	Type	Description	Parameters
DataTrickling.Enabled	Boolean	If true, data trickling is used for downloading web objects.	
DateTime.Date.MonthDayNumber	Number	Number of day in month	
DateTime.Date.MonthNumber	Number	Number of month	

Table A-8 List of properties – D *(continued)*

Name	Type	Description	Parameters
DateTime.Date.ToString	String	String representing current date (in the format specified by the property parameters)	String including the following three parts: 1 1. %YYYY (for the year) *or:* %YY (last two digits) *or:* %Y (last two digits, but only one digit if the last two digits begin with 0, for example, 9 for 2009) 2 %MM (for the month number with 0 inserted before one-digit numbers) *or:* %M (0 is not inserted, for example, 3 for March and 12 for December) 3 %DD (for the day) *or:* %D If no parameter is specified, the format is: %YYYY/%MM /%DD
DateTime.Date. WeekDayNumber	Number	Number of day in week (1 is Sunday)	
DateTime.Date.Year	Number	Year (four digits)	
DateTime.Date.YearTwoDigits	Number	Year (last two digits)	
DateTime.Time.Hour	Number	Hour (in 24-hours format, for example, 1 p. m. is 13)	
DateTime.Time.Minute	Number	Minute in hour	
DateTime.Time.Second	Number	Second in minute	

Table A-8 List of properties – D *(continued)*

Name	Type	Description	Parameters
DateTime.Time.ToString	String	String representing current time (in the format specified by the property parameters)	String including the following three parts: 1 1. %h (for the hour) *or:* %hh (with 0 inserted before a one-digit hour) 2 %m (for the minute) *or:* %mm 3 %s (for the second) *or:* %ss If no parameter is specified, the format is: %hh:%mm:%ss
DateTime.ToGMTString	String	String representing current date and time in Greenwich Mean Time format For example, "Mon, 22 March 2012 11:45:36 GMT"	
DateTime.ToISOString	String	String representating current date and time in ISO format For example, "2012-03-22 11:45:12"	
DateTime.ToNumber	Number	Number of seconds since beginning of 1/1/1970 (UNIX epoch time)	
DateTime.ToString	String	String representing current date and time (in the format specified by the property parameters)	String including the part of the *DateTime.Date.ToString* and *DateTime.Time. ToString* properties If no parameter is specified, the format is: %YYYY/%MM /%DD %hh:%mm:%ss
DateTime. ToWebReporterString	String	String representing current date and time in Web Reporter format For example, "29/Oct/ 2012:14:28:15 +0000"	

Table A-8 List of properties – D *(continued)*

Name	Type	Description	Parameters
DecimalNumber.ToString	String	Decimal number converted to a string The string is truncated according to a parameter. For example, 10.12345 is truncated to 10.12 if this parameter is 2.	1 Number: Decimal number to convert 2 Number: Number of places after the decimal point
Dimension.ToString	String	Dimension converted into a string	Dimension:Dimension to convert
DLP.Classification.AnyText. Matched	Boolean	If true, a given text string is specified as sensitive or inappropriate content by one or more entries in classification lists.	String: Text checked for being sensitive or inappropriate
DLP.Classification.AnyText. MatchedClassifications	List of String	List of entries in classification lists that specify a given text string as sensitive or inappropriate The list is filled when *DLP.Classification.AnyText.Matched* has been set to *true*.	String: Text checked for being sensitive or inappropriate
DLP.Classification.AnyText.. MatchedTerms	List of String	List of terms including a given text string that is specified as sensitive or inappropriate by one or more entries in classification lists The list is filled when *DLP.Classification.AnyText.Matched* has been set to *true*.	String: Text checked for being sensitive or inappropriate
DLP.Classification.BodyText. Matched	Boolean	If true, the text of a request or response body includes content that is specified as sensitive or inappropriate by one or more entries in classification lists.	
DLP.Classification.BodyText. MatchedClassifications	List of String	List of entries in classification lists that specify the sensitive or inappropiate content found in the body text of requests or responses The list is filled when *DLP.Classification.BodyText.Matched* has been set to *true* .	
DLP.Classification.BodyText. MatchedTerms	List of String	List of terms in request or response body text that are sensitive or inappropriate content according to one or more entries in classification lists. The list is filled when *DLP.Classification.BodyText.Matched* has been set to *true*.	
DLP.Dictionary.AnyText. Matched	Boolean	If true, a given text string is specified as sensitive or inappropriate content on a dictionary list.	String: Text checked for being sensitive or inappropriate

Table A-8 List of properties – D *(continued)*

Name	Type	Description	Parameters
DLP.Dictionary.AnyText.MatchedTerms	List of String	List of terms including a given text string that is specified as sensitive or inappropriate on a dictionary list The list is filled when *DLP.Dictionary .AnyText.Matched* has been set to *true*.	String: Text checked for being sensitive or inappropriate
DLP.Dictionary.BodyText.Matched	Boolean	If true, the text of a request or response body includes content that is specified as sensitive or inappropriate by an entry you made in a dictionary list.	
DLP.Dictionary.BodyText.MatchedTerms	List of String	List of the terms in request or response body text that are sensitive or inappropriate content according to the entries you made in a dictionary list The list is filled when *DLP.Dictionary.BodyText.Matched* has been set to *true*.	
DNS.Lookup	List of IP	List of IP addresses found in a DNS lookup for a host name	String: Host name
DNS.Lookup.Reverse	List of String	List of host names found in a reverse DNS lookup for an IP address	IP: IP address

Table A-9 List of properties – E

Name	Type	Description	Parameters
Error.ID	Number	ID of an error	
Error.Message	String	Message text describing an error	
ExtLists.Boolean	Boolean	Boolean value	1 String: Value holding the place of a term that identifies an external list source, for example, in a URL 2 String: as above 3 String: as above
ExtLists.Category	Category	URL category	as above
ExtLists.CategoryList	List of Category	List of URL categories	as above
ExtLists.Double	Double	Double value	as above
ExtLists.DoubleList	List of Double	List of Double values	as above
ExtLists.Integer	Integer	Integer	as above
ExtLists.IntegerList	List of Integer	List of integers	as above
ExtLists.IP	IP	IP address	as above
ExtLists.IPList	List of IP	List of IP addresses	as above
ExtLists.IPRange	IPRange	IP address range	as above
ExtLists.IPRangeList	List of IPRange	List of IP address ranges	as above

Table A-9 List of properties – E *(continued)*

Name	Type	Description	Parameters
ExtLists.LastUsedListName	String	String representing name of settings for the External Lists module that were used last	
ExtLists.MediaType	MediaType	Media type	as above
ExtLists.MediaTypeList	List of MediaType	List of media types	as above
ExtLists.String	String	String	as above
ExtLists.StringList	List of String	List of strings	as above
ExtLists.Wildcard	Wildcard Expression	Wildcard (regular) expression	as above
ExtLists.WildcardList	List of Wildcard Expression	List of wildcard (regular) expressions	as above

Table A-10 List of properties – F

Name	Type	Description	Parameters
FileSystemLogging. MakeAnonymous	String	String made anonymous by encryption	String: String to encrypt

Table A-11 List of properties – G

Name	Type	Description	Parameters
GTI.RequestSentToCloud	Boolean	If true, a lookup request for URL category information was sent to the Global Threat Intelligence server.	

Table A-12 List of properties – H

Name	Type	Description	Parameters
Header.Block.Exists	Boolean	If true, a specified block header exists.	String: Header name
Header.Block.Get	String	First value found for a specified block header	String: Header name
Header.Block.GetMultiple	List of String	List of values found for a specified block header	String: Header name
Header.Exists	Boolean	If true, a specified header is contained in a request or response that is processed on the appliance. It depends on the current processing cycle whether it is actually a request or response that contains the header.	String: Header name
Header.Get	String	First value found for the specified header in a request or response that is processed on the appliance It depends on the current processing cycle whether it is actually a request or response that contains the header.	String: Header name

Table A-12 List of properties – H *(continued)*

Name	Type	Description	Parameters
Header.GetMultiple	List of String	List of values found for a specified header in a request or response that is processed on the appliance It depends on the current processing cycle whether it is actually a request or response that contains the header.	String: Header name
Header.ICAP.Request.Exists	Boolean	If true, a specified header is contained in a request sent in ICAP communication.	String: Header name
Header.ICAP.Request.Get	String	First value found for a specified header in a request sent in ICAP communication	String: Header name
Header.ICAP.Response.Exists	Boolean	If true, a specified header is contained in a response received in ICAP communication.	String: Header name
Header.ICAP.Response.Get	String	First value found for a specified header in a response received in ICAP communication	String: Header name
Header.Request.Exists	Boolean	If true, a specified header is contained in a request.	String: Header name
Header.Request.Get	String	First value found for a specified header in a request	String: Header name
Header.Request.GetMultiple	List of String	List of values found for a specified header in a request	String: Header name
Header.Response.Exists	Boolean	If true, a specified header is contained in a response.	String: Header name
Header.Response.Get	String	First value found for a specified header in a response	String: Header name
Header.Response.GetMultiple	List of String	List of values found for a specified header in a response	String: Header name
Hex.ToString	String	Hex value converted into a string	Hex: Hex value to convert
HTML.Element.Attribute	String	String representing an attribute of an HTML element	
HTML.Element.Dimension	Dimension	Dimension of an HTML element (width and height)	
HTML.Element.HasAttribute	Boolean	If true, an HTML element has a specified attribute.	String: Attribute name
HTML.Element.Name	String	Name of an HTML element	
HTML.Element.ScriptType	String	Script type of an HTML element, for example, JavaScript or Visual Basic Script	

Table A-13 List of properties – I

Name	Type	Description	Parameters
ICAP.Policy	String	Name of a policy included in an ICAP request for a URL	
ICAP.ReqMod. ResponseHeader.Exists	Boolean	If true, a response sent from an ICAP server in REQMOD mode contains a specified header.	String: Header name

Table A-13 List of properties – I *(continued)*

Name	Type	Description	Parameters
ICAP.ReqMod.ResponseHeader.Get	String	First value found for a specified header in a REQMOD response	String: Header name
ICAP.ReqMod.ResponseHeader.GetMultiple	List of String	List of values found for a specified header in a REQMOD response	String: Header name
ICAP.ReqMod.Satisfaction	Boolean	If true, an ICAP server has replaced a request with a response. The ICAP server does this after sending a message that a particular request is blocked.	
ICAP.RespMod.EncapsulatedHTTPChanged	Boolean	If true, an ICAP server has changed the HTTP state for a response sent in RESPMOD mode.	
ICAP.RespMod.ResponseHeader.Exists	Boolean	If true, a response sent from an ICAP server in RESPMOD mode contains a specified header.	String: Header name
ICAP.RespMod.ResponseHeader.Get	String	First value found for a specified header in a RESPMOD response	String: Header name
ICAP.RespMod.ResponseHeader.GetMultiple	List of String	List of values found for a specified header in a RESPMOD response	String: Header name
IM.Direction	String	Direction of a chat message sent or a file transferred under an instant messaging protocol and processed on the appliance For a chat message sent from a client to the appliance, the direction could, for example, be specified as *out*, for a message sent from a server to the appliance it could be specified as *in*.	
IM.FileName	String	Name of a file transferred under an instant messaging protocol	
IM.FileSize	Number	Size of a file transferred under an instant messaging protocol (in bytes)	
IM.MessageCanSendBack	Boolean	If true, a block message or other message can be sent from the appliance to a user of an instant messaging service. A block message is, for example, sent back to a user who submitted a chat message during a time interval that is not allowed for chatting. A message can typically not be sent before a user has completed the procedure for logging on to the instant messaging service.	
IM.Notification	String	Name of a template used for sending a notification from the appliance to a user of an instant messaging service, for example, a block message	
IM.Recipient	String	Name of a client that receives a chat message or file under an instant messaging protocol This name can also be a group name (group ID) when a chat message is sent to a group of recipients.	
IM.Sender	String	Name of a client that sends a chat message or file under an instant messaging protocol	

Table A-13 List of properties – I *(continued)*

Name	Type	Description	Parameters
Incident.AffectedHost	IP	IP address of a host that is involved in an incident, for example, a web server that the appliance cannot connect to	
Incident.Description	String	Plain-text description of an incident	
Incident.ID	Number	ID of an incident For a list of these IDs, see the *List of incident IDs*.	
Incident.Origin	Number	Number specifying the appliance component that is the origin of an incident The following are some origin numbers that are presently in use: 1 – Appliance system 2 – Core subsystem 3 – Coordinator subsystem 4 – Anti-Malware process 5 – Log File Manager 6 – sysconf daemon 9 – Unidentified origin The origin of an incident is further specified by the *Incident.OriginName* property.	
Incident.OriginName	String	Name of an appliance component that is the origin of an incident The origin name can also specify a subcomponent that is a part of the component specified by the origin number. For example, origin number 2 (Core) can be further specified by the origin name as: • Core • Proxy • Anti-Malware Filter • URL Filter • and other names of subcomponents	

Table A-13 List of properties – I *(continued)*

Name	Type	Description	Parameters
Incident.Severity	Number	Severity of an incident Severity levels: 0 – Emergency 1 – Alert 2 – Critical 3 – Error 4 – Warning 5 – Notice 6 – Informational 7 – Debug These levels are the same as those used in syslog entries.	
IP.ToString	String	IP address converted into a string	IP: IP address to convert
IPRange.ToString	String	Range of IP addresses converted into a string	IPRange: Range of IP addresses to convert

Table A-14 List of properties – L

Name	Type	Description	Parameters
License.RemainingDays	Number	Remaining time until a license expires (in days)	
List.LastMatches	String	String containing all elements that have been found to match when two lists are compared using an operator such as *at least one in list* or *all in list* Matches are only added to the list as long it has not yet been decided whether the relationship between the lists that the operator evaluates exists or not. For example, list A contains the elements 1, 2, 3, whereas list B contains 1, 2, 4. Both lists are compared using the *at least one in list* operator. To find out that list A actually contains at least one element of list B, the operator only needs to compare element 1 in both lists and detect that they match. *List.LastMatches* then contains 1 because it has been found to be a match. 2 is also a match in the two lists, but is not contained in *List.LastMatches* because it was not evaluated by the operator and found to be a match. This was not done because the operator had already found out after evaluating the 1 in both lists that at least one element of list A was also in list B.	
List.OfCategory.Append	List of Category	List of URL categories that a category is appended to	1 List of Category: List to append category to 2 Category: Category to append
List.OfCategory.ByName	List of Category	List of URL categories (specified by its name)	String: List name

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfCategory.Erase	List of Category	List of URL categories with specified category erased	1 List of Category: List with category to erase 2 Number: Position of category to erase
List.OfCategory.EraseElementRange	List of Category	List of URL categories with specified range of categories erased	1 List of Category: List with categories to erase 2 Number: Position of first category to erase 3 Number: Position of last category to erase
List.OfCategory.EraseList	List of Category	List of URL categories with categories that are also on other list erased	1 List of Category: List with categories to erase 2 List of Category: List of categories to erase on first list
List.OfCategory.Find	Number	Position of a URL category on a list	1 List of Category: List with category to find position for 2 Category: Category to find position for
List.OfCategory.Get	Category	URL category specified by its position on a list	1 List of Category: List containing category 2 Number: Position of category on list
List.OfCategory.GetElementRange	List of Category	List of URL categories extracted from other list 1 List of Category: List with categories to extract 2 Number: Position of first category to extract 3 Number: Position of last category to extract	1 List of Category: List with categories to extract 2 Number: Position of first category to extract 3 Number: Position of last category to extract
List.OfCategory.Insert	List of Category	List of URL categories with specified category inserted	1 List of Category: List to insert category in 2 Category: Category to insert
List.OfCategory.IsEmpty	Boolean	If true, the specified list is empty.	List of Category: List to check for being empty

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfCategory.Join	List of Category	List of URL categories created by joining two lists	1 List of Category: First list to join 2 List of Category: Second list to join
List.OfCategory.Reverse	List of Category	List of URL categories that has its original order reverted	List of Category: List in original order
List.OfCategory.Size	Number	Number of URL categories on a list	List of Category: List to provide number of categories for
List.OfCategory.Sort	List of Category	List of URL categories sorted in alphabetical order	List of Category: List to sort
List.OfCategory.ToShortString	String	List of URL categories converted into a list of their abbreviated name forms	List of Category: List to convert
List.OfCategory.ToString	String	List of URL categories converted into a string	List of Category: List to convert
List.OfDimension.Append	List of Dimension	List of dimensions that a dimension is appended to	1 List of Dimension: List to append dimension to 2 Dimension: Dimension to append
List.OfDimension.ByName	List of Dimension	List of dimensions specified by its name	String: List name
List.OfDimension.Erase	List of Dimension	List of dimensions with specified dimension erased	1 List of Dimension: List with dimension to erase 2 Number: Position of dimension to erase
List.OfDimension. EraseElementRange	List of Dimension	List of dimensions with specified range of dimensions erased	1 List of Dimension: List with dimension range to erase 2 Number: Position of first dimension to erase 3 Number: Position of last dimension to erase
List.OfDimension.EraseList	List of Dimension	List of dimensions with dimensions that are also on other list erased	1 List of Dimension: List with dimensions to erase 2 List of Dimension: List of dimensions to erase on first list

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfDimension.Find	Number	Position of a dimension on a list	1 List of Dimension: List with dimension to find position for 2 Dimension: Dimension to find position for
List.OfDimension.Get	Dimension	Dimension specified by its position on a list	1 List of Dimension: List containing dimension 2 Number: Position of dimension on list
List.OfDimension.GetElementRange	List of Dimension	List of dimensions extracted from other list	1 List of Dimension: List with dimensions to extract 2 Number: Position of first dimension to extract 3 Number: Position of last dimension to extract 4 Dimension: Dimension to insert
List.OfDimension.Insert	List of Dimension	List of dimensions with specified dimension inserted	1 List of Dimension: List to insert dimension in 2 Dimension: Dimension to insert
List.OfDimension.IsEmpty	Boolean	If true, the specified list is empty.	List of Dimension: List to check for being empty
List.OfDimension.Join	List of Dimension	List of dimensions created by joining two lists	1 List of Dimension: First list to join 2 List of Dimension: Second list to join
List.OfDimension.Reverse	List of Dimension	List of dimensions that has its original order reverted	List of Dimension: List in original order
List.OfDimension.Size	Number	Number of dimensions on a list	List of Dimension: List to provide number of dimensions for
List.OfDimension.Sort	List of Dimension	List of dimensions sorted in alphabetical order	List of Dimension: List to sort
List.OfDimension.ToString	String	List of dimensions converted into a string	List of Dimension: List to convert
List.OfHex.Append	List of Hex	List of hex values that a hex value is appended to	1 List of Hex: List to append Hex value to 2 Hex: Hex value to append
List.OfHex.ByName	List of Hex	List of hex values specified by its name	String: List name

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfHex.Erase	List of Hex	List of hex values with specified value erased	1 List of Hex: List with hex value to erase 2 Number: Position of hex value to erase
List.OfHex.EraseElementRange	List of Hex	List of hex values with specified range of values erased	1 List of Hex: List with hex values to erase 2 Number: Position of first hex value to erase 3 Number: Position of last hex value to erase
List.OfHex.EraseList	List of Hex	List of hex values with values that are also on other list erased	1 List of Hex: List with hex values to erase 2 List of Hex: List of hex values to erase on first list
List.OfHex.Find	Number	Position of a hex value on a list	1 List of Hex: List with hex value to find position for 2 Hex: Hex value to find position for
List.OfHex.Get	Hex	Hex value specified by its position on a list	1 List of Hex: List containing hex value 2 Number: Position of hex value on list
List.OfHex.GetElementRange	List of Hex	List of hex values extracted from other list	1 List of Hex: List with hex values to extract 2 Number: Position of first hex value to extract 3 Number: Position of last hex value to extract
List.OfHex.Insert	List of Hex	List of hex values with specified value inserted	1 List of Hex: List to insert hex value in 2 Hex: Hex value to insert
List.OfHex.IsEmpty	Boolean	If true, the specified list is empty.	List of Hex: List to check for being empty
List.OfHex.Join	List of Hex	List of hex values created by joining two lists	1 List of Hex: First list to join 2 List of Hex: Second list to join
List.OfHex.Reverse	List of Hex	List of hex values that has its original order reverted	List of Hex: List in original order

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfHex.Size	Number	Number of hex values on a list	List of Hex: List to provide number of hex values for
List.OfHex.Sort	List of Hex	List of sorted hex values	List of Hex: List to sort
List.OfHex.ToString	String	List of hex values converted into a string	List of Hex: List to convert
List.OfIP.Append	List of IP	List of IP addresses that an IP address is appended to	**1** List of IP: List to append IP address to **2** IP: IP address to append
List.OfIP.ByName	List of IP	List of IP addresses (specified by its name)	String: List name
List.OfIP.Erase	List of IP	List of IP addresses with specified address erased	**1** List of IP: List with IP address to erase **2** Number: Position of IP address to erase
List.OfIP.EraseElementRange	List of IP	List of IP addresses with specified range of addresses erased	**1** List of IP: List with IP addresses to erase **2** Number: Position of first IP address to erase **3** Number: Position of last IP address to erase
List.OfIP.EraseList	List of IP	List of IP addresses with addresses that are also on other list erased	**1** List of IP: List with IP addresses to erase **2** List of IP: List of IP addresses to erase on first list
List.OfIP.Find	Number	Position of an IP address on a list	**1** List of IP: List with IP address to find position for **2** IP: IP address to find position for
List.OfIP.Get	IP	IP address specified by its position on a list	**1** List of IP: List containing IP address **2** Number: Position of IP address on list
List.OfIP.GetElementRange	List of IP	List of IP addresses extracted from another list	**1** List of IP: List with IP addresses to extract **2** Number: Position of first IP address to extract **3** Number: Position of last IP address to extract

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfIP.Insert	List of IP	List of IP addresses with specified address inserted	1 List of IP: List to insert IP address in 2 IP: IP address to insert
List.OfIP.IsEmpty	Boolean	If true, the specified list is empty.	List of IP: List to check for being empty
List.OfIP.Join	List of IP	List of IP addresses created by joining two lists	1 List of IP: First list to join 2 List of IP: Second list to join
List.OfIP.Reverse	List of IP	List of IP addresses that has its original order reverted	List of IP: List in original order
List.OfIP.Size	Number	Number of IP addresses on a list	List of IP: List to provide number of IP addresses for
List.OfIP.Sort	List of IP	List of sorted IP addresses	List of IP: List to sort
List.OfIP.ToString	String	List of IP addresses converted into a string	List of IP: List to convert
List.OfIPRange.Append	List of IPRange	List of IP address ranges that an IP address range is appended to	1 List of IPRange: List to append IP address range to 2 IPRange: IP address range to append
List.OfIPRange.ByName	List of IPRange	List of IP address ranges specified by its name	String: List name
List.OfIPRange.Erase	List of IPRange	List of IP address ranges with specified range erased	1 List of IPRange: List with IP address range to erase 2 Number: Position of IP address range to erase
List.OfIPRange. EraseElementRange	List of IPRange	List of IP address ranges with specified ranges erased	1 List of IPRange: List with IP address ranges to erase 2 Number: Position of first IP address range to erase 3 Number: Position of last IP address range to erase
List.OfIPRange.EraseList	List of IPRange	List of IP address ranges with ranges that are also on other list erased	1 List of IPRange: List with IP address ranges to erase 2 List of IPRange: List of IP address ranges to erase on first list

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfIPRange.Find	Number	Position of an IP address range on a list	1 List of IPRange: List with IP address range to find position for 2 IPRange: IP address range to find position for
List.OfIPRange.Get	IPRange	IP address range specified by its position on a list	1 List of IPRange: List containing IP address range 2 Number: Position of IP address range on list
List.OfIPRange.GetElementRange	List of IPRange	List of IP address ranges extracted from other list	1 List of IPRange: List with IP address ranges to extract 2 Number: Position of first IP address range to extract 3 Number: Position of last IP address range to extract
List.OfIPRange.Insert	List of IPRange	List of IP address ranges with specified range inserted	1 List of IPRange: List to insert IP address range in 2 IPRange: IP address range to insert
List.OfIPRange.IsEmpty	Boolean	If true, the specified list is empty.	List of IPRange: List to check for being empty
List.OfIPRange.Join	List of IPRange	List of IP address ranges created by joining two lists	1 List of IPRange: First list to join 2 List of IPRange: Second list to join
List.OfIPRange.Reverse	List of IPRange	List of IP address rangess that has its original order reverted	List of IPRange: List in original order
List.OfIPRange.Size	Number	Number of IP address ranges on a list	List of IPRange: List to provide number of IP address ranges for
List.OfIPRange.Sort	List of IPRange	List of sorted IP address ranges	List of IPRange: List to sort
List.OfIPRange.ToString	String	List of IP address ranges converted into a string	List of IPRange: List to convert
List.OfMediaType.Append	List of MediaType	List of media types that a media type is appended to	1 List of MediaType: List to append media type to 2 MediaType: Media type to append

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfMediaType.ByName	List of MediaType	List of media types specified by its name	String: List name
List.OfMediaType.Erase	List of MediaType	List of media types with specified type erased	1 List of MediaType: List with media type to erase 2 Number: Position of media type to erase
List.OfMediaType.EraseElementRange	List of MediaType	List of media types with specified range of types erased	1 List of MediaType: List with media types to erase 2 Number: Position of first media type to erase 3 Number: Position of last media type to erase
List.OfMediaType.EraseList	List of MediaType	List of media types with types that are also on other list erased	1 List of MediaType: List with media types to erase 2 List of MediaType: List of media types to erase on first list
List.OfMediaType.Find	Number	Position of a media type on a list	1 List of MediaType: List with media type to find position for 2 MediaType: Media type to find position for
List.OfMediaType.Get	MediaType	Media type specified by its position on a list	1 List of MediaType: List containing media type 2 Number: Position of media type on list
List.OfMediaType.GetElems	List of MediaType	List of media types extracted from other list	1 List of MediaType: List with media types to extract 2 Number: Position of first media type to extract 3 Number: Position of last media type to extract
List.OfMediaType.Insert	List of MediaType	List of media types with specified type inserted	1 List of MediaType: List to insert media type in 2 MediaType: Media type to insert
List.OfMediaType.IsEmpty	Boolean	If true, the specified list is empty.	List of MediaType: List to check for being empty

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfMediaType.Join	List of MediaType	List of media types created by joining two lists	1 List of MediaType: First list to join 2 List of MediaType: Second list to join
List.OfMediaType.Reverse	List of MediaType	List of media types that has its original order reverted	List of MediaType: List in original order
List.OfMediaType.Size	Number	Number of media types on a list	List of MediaType: List to provide number of media types for
List.OfMediaType.Sort	List of MediaType	List of media types sorted in alphabetical order	List of MediaType: List to sort
List.OfMediaType.ToString	String	List of media types converted into a string	List of MediaType: List to convert
List.OfNumber.Append	List of Number	List of numbers that a number is appended to	1 List of Number: List to append number to 2 Number: Number to append
List.OfNumber.ByName	List of Number	List of numbers specified by its name	String: List name
List.OfNumber.Erase	List of Number	List of numbers with specified number erased	1 List of Number: List with number to erase 2 Number: Position of number to erase
List.OfNumber. EraseElementRange	List of Number	List of numbers with specified range of numbers erased	1 List of Number: List with numbers to erase 2 Number: Position of first number to erase 3 Number: Position of last number to erase
List.OfNumber.EraseList	List of Number	List of numbers with numbers that are also on other list erased	1 List of Number: List with numbers to erase 2 List of Number: List of numbers to erase on first list
List.OfNumber.Find	Number	Position of a number on a list	1 List of Number: List with number to find position for 2 Number: Number to find position for

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfNumber.Get	Number	Number specified by its position on a list	1 List of Number: List containing number 2 Number: Position of number on list
List.OfNumber.GetElementRange	List of Number	List of numbers extracted from other list	1 List of Number: List with numbers to extract 2 Number: Position of first number to extract 3 Number: Position of last number to extract
List.OfNumber.Insert	List of Number	List of numbers with specified number inserted	1 List of Number: List to insert number in 2 Number: Number to insert
List.OfNumber.IsEmpty	Boolean	If true, the specified list is empty.	List of Number: List to check for being empty
List.OfNumber.Join	List of Number	List of numbers created by joining two lists	1 List of Number: First list to join 2 List of Number: Second list to join
List.OfNumber.Reverse	List of Number	List of numbers that has its original order reverted	List of Number: List in original order
List.OfNumber.Size	Number	Number of numbers on a list	List of Number: List to provide number of numbers for
List.OfNumber.Sort	List of Number	List of sorted numbers	List of Number: List to sort
List.OfNumber.ToString	String	List of numbers converted into a string	List of Number: List to convert
List.OfString.Append	List of String	List of strings that a string is appended to	1 List of String: List to append string to 2 String: String to append
List.OfString.ByName	List of String	List of strings specified by its name	String: List name
List.OfString.Erase	List of String	List of strings with specified string erased	1 List of String: List with string to erase 2 Number: Position of string to erase

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfString. EraseElementRange	List of String	List of strings with specified range of strings erased	1 List of String: List with strings to erase 2 Number: Position of first string to erase 3 Number: Position of last string to erase
List.OfString.EraseList	List of String	List of strings with strings that are also on other list erased	1 List of String: List with strings to erase 2 List of String: List of strings to erase on first list
List.OfString.Find	Number	Position of a string on a list	1 List of String: List with string to find position for 2 String: String to find position for
List.OfString.Get	String	String specified by its position on a list	1 List of String: List containing string 2 Number: Position of string on list
List.OfString.GetElementRang e	List of String	List of strings extracted from other list	1 List of String: List with strings to extract 2 Number: Position of first string to extract 3 Number: Position of last string to extract
List.OfString.Insert	List of String	List of strings with specified string inserted	1 List of String: List to insert number in 2 String: String to insert
List.OfString.IsEmpty	Boolean	If true, the specified list is empty	List of String: List to check for being empty
List.OfString.Join	List of String	List of strings created by joining two lists	1 List of String: First list to join 2 List of String: Second list to join

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfStringMapInList	List of String	String specified by a parameter and contained in a list with an index for the position this string has in another list If the specified string is not contained in the first list or does not exist as a position in the second list, the string is empty.	1 List of String: First list containing string 2 List of String: Second list containing string 3 String: String contained in first and second list or empty string
List.OfString.Reverse	List of String	List of strings that has its original order reverted	List of String: List in original order
List.OfString.Size	Number	Number of strings on a specified list	List of String: List to provide number of strings for
List.OfString.Sort	List of String	List of strings sorted in alphabetical order	List of String: List to sort
List.OfString.ToString	String	List of strings converted into a string	List of String: List to convert
List.OfWildcard.Append	List of Wildcard Expression	List of wildcard expressions that an expression is appended to	1 List of Wildcard Expression: List to append wildcard expression to 2 Wildcard Expression: Wildcard expression to append
List.OfWildcard.ByName	List of Wildcard Expression	List of wildcard expressions specified by its name	String: List name
List.OfWildcard.Erase	List of Wildcard Expression	List of wildcard expressions with specified expression erased	1 List of Wildcard Expression: List with wildcard expression to erase 2 Number: Position of wildcard expression to erase
List.ofWildcard. EraseElementRange	List of Wildcard Expression	List of wildcard expressions with specified range of expressions erased	1 List of Wildcard Expression: List with wildcard expressions to erase 2 Number: Position of first wildcard expression to erase 3 Number: Position of last wildcard expression to erase

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfWildcard.EraseList	List of Wildcard Expression	List of wildcard expressions with expressions that are also on other list erased	1 List of Wildcard Expression: List with wildcard expressions to erase 2 List of Wildcard Expression: List of wildcard expressions to erase on first list
List.OfWildcard.Find	Number	Position of a wildcard expression on a list	1 List of Wildcard expression: List with wildcard expression to find position for 2 Wildcard expression: Wildcard expression to find position for
List.OfWildcard.Get	Wildcard Expression	Wildcard expression specified by its position on a list	1 List of Wildcard Expression: List containing wildcard expression 2 Number: Position of wildcard expression on list
List.OfWildcard.GetElementRange	List of Wildcard Expression	List of wildcard expressions extracted from other list	1 List of Wildcard Expression: List with wildcard expressions to extract 2 Number: Position of first wildcard expression to extract 3 Number: Position of last wildcard expression to extract
List.OfWildcard.Insert	List of Wildcard Expression	List of wildcard expressions with specified expression inserted	1 List of Wildcard Expression: List to insert wildcard expression in 2 Wildcard Expression: Wildcard expression to insert
List.OfWildcard.IsEmpty	Boolean	If true, the specified list is empty.	List of Wildcard Expression: List to check for being empty

Table A-14 List of properties – L *(continued)*

Name	Type	Description	Parameters
List.OfWildcard.Join	List of Wildcard Expression	List of wildcard expressions created by joining two lists	1 List of Wildcard Expression: First list to join 2 List of Wildcard Expression: Second list to join
List.OfWildcard.Reverse	List of Wildcard Expression	List of wildcard expressions that has its original order reverted	List of Wildcard Expression: List in original order
List.OfWildcard.Size	Number	Number of wildcard expressions on a list	List of Wildcard Expression: List to provide number of wildcard expressions for
List.OfWildcard.Sort	List of Wildcard Expression	List of sorted wildcard expressions	List of Wildcard Expression: List to sort
List.OfWildcard.ToString	String	List of wildcard expressions converted into a string	List of Wildcard Expression: List to convert

Table A-15 List of properties – M

Name	Type	Description	Parameters
Math.Abs	Number	Absolute value of specified number	Number: Number that absolute value is provided for
Math.Random	Number	Random number between specified minimum and maximum values (including these values)	1 Number: Minimum value 2 Number: Maximum value
MediaStreamProbability	Number	Probability that the streaming media in question matches the found media type (in percent)	
MediaType.EnsuredTypes	List of MediaType	List of media types that are ensured for the respective media with a probability of more than 50%	
MediaType.FromFileExtension	List of MediaType	List of media types that are found using the file name extension of the media	
MediaType.FromHeader	List of MediaType	List of media types that are found using the content-type header sent with the media	
MediaType.HasOpener	Boolean	If true, an opener module is available on the appliance for media of a given type.	
MediaType.IsCompositeObject	Boolean	If true, media of a given type is a composite object, for example, is an archive.	

Table A-15 List of properties – M *(continued)*

Name	Type	Description	Parameters
MediaType. MagicBytesMismatch	Boolean	If true, the media type specified in the header sent with the media does not match the type that was found on the appliance by examining the magic bytes actually contained in the media.	
MediaType.NotEnsuredTypes	List of MediaType	List of media types that are ensured for the respective media with a probability of less than 50%	
MediaType.ToString	String	Media type converted into a string	MediaType: Media type to convert
Message.Language	String	Name of language for messages sent to users in short form, for example, en, de, ja	
Message.TemplateName	String	Name of a template for messages sent to users	

Table A-16 List of properties – N

Name	Type	Description	Parameters
Number.ToDecimalNumber	Number	Integer converted into decimal format For example, 10 is converted to 10.0.	Number: Integer to convert
Number.ToString	String	Number converted into a string	Number: Number to convert
Number.ToVolumeString	String	Number of bytes that a volume amounts to converted into a string	Number: Number of bytes to convert
NumberOfClientConnections	Number	Number of connections to clients that are open on an appliance at the same time	

Table A-17 List of properties – P

Name	Type	Description	Parameters
PDStorage.GetAllData	List of String	List containing all permanently stored data in string format	
PDStorage.GetAllGlobalData	List of String	List containing all permanently stored global data in string format	
PDStorage.GetAllUserData	List of String	List containing all permanently stored user data in string format	
PDStorage.GetGlobalData.Bool	Boolean	Global variable of type Boolean	String: Variable key
PDStorage.GetGlobalData. Category	Category	Global variable of type Category	String: Variable key
PDStorage.GetGlobalData. Dimension	Dimension	Global variable of type Dimension	String: Variable key
PDStorage.GetGlobalData.Hex	Hex	Global variable of type Hex	String: Variable key
PDStorage.GetGlobalData.IP	IP	Global variable of type IP	String: Variable key

Table A-17 List of properties – P *(continued)*

Name	Type	Description	Parameters
PDStorage.GetGlobalData. IPRange	IPRange	Global variable of type IPRange	String: Variable key
PDStorage.GetGlobalData.List. Category	List of Category	Global variable of type List of Category	String: Variable key
PDStorage.GetGlobalData. List. Dimension	List of Dimension	Global variable of type List of Dimension	String: Variable key
PDStorage.GetGlobalData. List Hex	List of Hex	Global variable of type List of Hex	String: Variable key
PDStorage.GetGlobalData.List. IP	List of IP	Global variable of type List of IP	String: Variable key
PDStorage.GetGlobalData.List. IPRange	List of IPRange	Global variable of type List of IPRange	String: Variable key
PDStorage.GetGlobalData.List. MediaType	List of MediaType	Global variable of type List of MediaType	String: Variable key
PDStorage.GetGlobalData.List. Number	List of Number	Global variable of type List of Number	String: Variable key
PDStorage.GetGlobalData.List. String	List of String	Global variable of type List of String	String: Variable key
PDStorage.GetGlobalData.List. WildcardExpression	List of Wildcard Expression	Global variable of type List of WildcardExpression	String: Variable key
PDStorage.GetGlobalData. MediaType	MediaType	Global variable of type MediaType	String: Variable key
PDStorage.GetGlobalData. Number	Number	Global variable of type Number	String: Variable key
PDStorage.GetGlobalData. String	String	Global variable of type String	String: Variable key
PDStorage.GetGlobalData. WildcardExpression	Wildcard Expression	Global variable of type WildcardExpression	String: Variable key
PDStorage.GetUserData.Bool	Boolean	User variable of type Boolean	String: Variable key
PDStorage.GetUserData. Category	Category	User variable of type Category	String: Variable key
PDStorage.GetUserData. Dimension	Dimension	User variable of type Dimension	String: Variable key
PDStorage.GetUserData.Hex	Hex	User variable of type Hex	String: Variable key
PDStorage.GetUserData.IP	IP	User variable of type IP	String: Variable key
PDStorage.GetUserData. IPRange	IPRange	User variable of type IPRange	String: Variable key
PDStorage.GetUserData.List Category	List of Category	User variable of type List of Category	String: Variable key
PDStorage.GetUserData.List Dimension	List of Dimension	User variable of type List of Dimension	String: Variable key
PDStorage.GetUserData.List Hex	List of Hex	User variable of type List of Hex	String: Variable key

Table A-17 List of properties – P *(continued)*

Name	Type	Description	Parameters
PDStorage.GetUserData.List IP	List of IP	User variable of type List of IP	String: Variable key
PDStorage.GetUserData.List IPRange	List of IPRange	User variable of type List of IPRange	String: Variable key
PDStorage.GetUserData.List MediaType	List of MediaType	User variable of type List of MediaType	String: Variable key
PDStorage.GetUserData.List String	List of Number	User variable of type List of Number	String: Variable key
PDStorage.GetUserData.List Category	List of String	User variable of type List of String	String: Variable key
PDStorage.GetUserData. ListWildcard Expression	List of Wildcard Expression	User variable of type List of WildcardExpression	String: Variable key
PDStorage.GetUserData. MediaType	MediaType	User variable of type MediaType	String: Variable key
PDStorage.GetUserData. Number	Number	User variable of type Number	String: Variable key
PDStorage.GetUserData. String	String	User variable of type String	String: Variable key
PDStorage.GetUserData. WildcardExpression	Wildcard Expression	User variable of type WildcardExpression	String: Variable key
PDStorage.HasGlobalData	Boolean	If true, permanently stored global data is available.	String: Variable key
PDStorage.HasGlobalDataWait	Boolean	If true, a request is kept waiting until the requested global variable exists in the storage or the specified time interval has elapsed. The value of the property is then set to false. It is true by default.	1 String: Variable key 2 Number: Timeout (in seconds)
PDStorage.HasUserData	Boolean	If true, permanently stored user data is available.	String: Variable key
ProgressPage.Enabled	Boolean	If true, download progress is indicated to the user by a progress page.	
Protocol.FailureDescription	String	String containing description of a connection error under the current protocol	
Proxy.EndUserURL	String	String representing URL for display to a user	
Proxy.IP	IP	IP address of a connection	
Proxy.Port	Number	Number of port used for a connection	

Table A-18 List of properties – Q

Name	Type	Description	Parameters
Quota.AuthorizedOverride. GetLogin	String	User name submitted for performing an authorized override	
Quota.AuthorizedOverride. IsActivationRequest	Boolean	If true, an authorized user has chosen to continue with a authorized override session after session time has been exceeded.	
Quota.AuthorizedOverride. IsActivationRequest.Strict	Boolean	If true, an authorized user has chosen to continue with an Authorized Override session and the request for continuing the session applies to the current settings.	
Quota.AuthorizedOverride.JS. ActivateSession	String	String in JavaScript code calling the function that is executed when an authorized user chooses to start a new session by clicking the appropriate button in the authorized override template. The code is provided when the template is created and displayed to the user.	
Quota.AuthorizedOverride. RemainingSession	Number	Remaining time (in seconds) for an authorized override session	
Quota.AuthorizedOverride. SessionExceeded	Boolean	If true, the time allowed for an authorized override session has been exceeded.	
Quota.AuthorizedOverride. SessionLength	Number	Time length (in seconds) for an authorized override session	
Quota.Coaching. IsActivationRequest	Boolean	If true, a user has chosen to continue with a new coaching session after session time has been exceeded.	
Quota.Coaching. IsActivationRequest.Strict	Boolean	If true, a user has chosen to continue with a Coaching session and the request for continuing the session applies to the current settings.	
Quota.Coaching.JS. ActivateSession	String	String in JavaScript code calling the function that is executed when a user chooses to start a new session by clicking the appropriate button in the coaching session template. The code is provided when the template is created and displayed to the user.	
Quota.Coaching. RemainingSession	Number	Remaining time (in seconds) for a coaching session	
Quota.Coaching. SessionExceeded	Boolean	If true, the time allowed for a coaching session has been exceeded.	
Quota.Coaching.SessionLength	Number	Time length (in seconds) for a coaching session	
Quota.Time.Exceeded	Boolean	If true, the time quota has been exceeded.	
Quota.Time. IsActivationRequest	Boolean	If true, a user has chosen to continue with a new time session after session time has been exceeded.	

Table A-18 List of properties – Q *(continued)*

Name	Type	Description	Parameters
Quota.Time. IsActivationRequest.Strict	Boolean	If true, a user has chosen to continue with a new Time session and the request for continuing the session applies to the current settings.	
Quota.Time.JS. ActivateSession	String	String in JavaScript code calling the function that is executed when a user chooses to start a new session by clicking the appropriate button in the time session template. The code is provided when the template is created and displayed to the user.	
Quota.Time.RemainingDay	Number	Time (in seconds) remaining from the configured time quota for the current day	
Quota.Time.RemainingDay. ReducedAtActivation	Number	Time (in seconds) remaining from the configured time quota for the current day when a user has just started a session	
Quota.Time.RemainingDay. ReducedAtDeactivation	Number	Time (in seconds) remaining from the configured time quota for the current day when a user has just closed a session	
Quota.Time.RemainingMonth	Number	Time (in seconds) remaining from the configured time quota for the current month	
Quota.Time.RemainingMonth. ReducedAtActivation	Number	Time (in seconds) remaining from the configured time quota for the current month when a user has just started a session	
Quota.Time.RemainingMonth. ReducedAtDeactivation	Number	Time (in seconds) remaining from the configured time quota for the current month when a user has just closed a session	
Quota.Time.RemainingSession	Number	Remaining time (in seconds) for a time session	
Quota.Time.RemainingWeek	Number	Time (in seconds) remaining from the configured time quota for the current week	
Quota.Time.RemainingWeek. ReducedAtActivation	Number	Time (in seconds) remaining from the configured time quota for the current week when a user has just started a session	
Quota.Time.RemainingWeek. ReducedAtDeactivation	Number	Time (in seconds) remaining from the configured time quota for the current week when a user has just started a session	
Quota.Time.SessionExceeded	Boolean	If true, the time allowed for a time session has been exceeded.	
Quota.Time.SessionLength	Number	Time length (in seconds) for a time session	
Quota.Time.SizePerDay	Number	Time (in seconds) allowed per day under the configured quota	
Quota.Time.SizePerMonth	Number	Time (in seconds) allowed per month under the configured quota	

Table A-18 List of properties – Q *(continued)*

Name	Type	Description	Parameters
Quota.Time.SizePerWeek	Number	Time (in seconds) allowed per week under the configured quota	
Quota.Volume.Exceeded	Boolean	If true, the volume quota has been exceeded.	
Quota.Volume. IsActivationRequest	Boolean	If true, a user has chosen to continue with a new volume session after session time has been exceeded.	
Quota.Volume. IsActivationRequest.Strict	Boolean	If true, a user has chosen to continue a session when the configured volume has been exceeded and the request for continuing the session applies to the current settings.	
Quota.Volume.JS. ActivateSession	String	String in JavaScript code calling the function that is executed when a user chooses to start a new session by clicking the appropriate button in the volume session template. The code is provided when the template is created and displayed to the user.	
Quota.Volume.RemainingDay	Number	Volume (in bytes) remaining from the configured volume quota for the current day	
Quota.Volume. RemainingMonth	Number	Volume (in bytes) remaining from the configured volume quota for the current month	
Quota.Volume. RemainingSession	Number	Remaining time (in seconds) for a volume session	
Quota.Volume.RemainingWeek	Number	Volume (in bytes) remaining from the configured volume quota for the current week	
Quota.Volume.SessionExceeded	Boolean	If true, the time allowed for a volume session has been exceeded.	
Quota.Volume.SessionLength	Number	Time length (in seconds) for a volume session	
Quota.Volume.SizePerDay	Number	Volume (in bytes) allowed per day under the configured quota	
Quota.Volume.SizePerMonth	Number	Volume (in bytes) allowed per month under the configured quota	
Quota.Volume.SizePerWeek	Number	Volume (in bytes) allowed per week under the configured quota	

Table A-19 List of properties – R

Name	Type	Description	Parameters
Redirect.URL	String	String representing a URL that a user is redirected to by an authentication or quota rule	
Reporting.URL.Categories	List of Category	List of all URL categories used on the appliance	
Reporting.URL.Reputation	List of Number	List of all reputation score values used on the appliance	

Table A-19 List of properties – R *(continued)*

Name	Type	Description	Parameters
Request.Header.FirstLine	String	First line of a header sent with a request	
Request.ProtocolAndVersion	String	Protocol and protocol version used when a request is sent	
Response.ProtocolandVersion	String	Protocol and protocol version used when a response is sent	
Response.Redirect.URL	String	URL that a user is redirected to when aresponse is sent	
Response.StatusCode	String	Status code of a response	
Rules.CurrentRuleID	String	ID of the rule that is currently processed	
Rules.CurrentRuleName	String	Name of the rule that is currently processed	
Rules.CurrentRuleSetName	String	Name of the rule set that is currently processed	
Rules.EvaluatedRules	List of String	List of all rules that have been processed	
Rules.EvaluatedRules.Names	List of String	List with names of all rules that have been processed	
Rules.FiredRules	List of String	List of all rules that have applied	
Rules.FiredRules.Names	List of String	List with names of all rules that have applied	

Table A-20 List of properties – S

Name	Type	Description	Parameters
SecureReverseProxy. EmbeddedHost	String	Host name of a URL in an HTTP request that is embedded in an HTTPS request	
SecureReverseProxy. Embedded Protocol	String	Protocol of a URL in an HTTP request that is embedded in an HTTPS request	
SecureReverseProxy. Embedded URL	String	URL in an HTTP request that is embedded in an HTTPS request This is the URL for the host specified by the value of the *SecureReverseProxy.EmbeddedHost* property.	String: Host name of the URL
SecureReverseProxy. GetDomain	String	Domain specified in the settings for the SecureReverseProxy module	
SecureReverseProxy. IsValidReverseProxyRequest	Boolean	If true, the URL submitted in a request has the format required in a SecureReverseProxy configuration.	
SecureReverseProxy. URLToEmbed	String	URL submitted in a HTTP request that is embedded in an HTTPS request	

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
SecureToken.CreateToken	String	Encrypted string This string serves as a token for securing an IP address. An AES-128-bit algorithm is used to create the token. Depending on the value of a parameter in the settings of the SecureReverseProxy module, the string includes a time stamp.	String: String to encrypt
SecureToken.IsValid	Boolean	If true, the specified token is valid and has not expired. Depending on the on the value of a parameter in the settings of the SecureReverse Proxy module, the token string includes no time stamp. Expiration of the token is then not checked.	1 String: Token to be checked 2 Number: Time (in seconds) to elapse until the token expires
SecureToken.GetString	String	String serving as a token for securing an IP address If the token is invalid or has expired, the string is empty.	1 String: Token to be checked 2 Number: Time (in seconds) to elapse until the token expires
SNMP.Trap.Additional	String	Additional message sent to a trap under the SNMP protocol	
SSL.Certificate. CN.ToWildcard	Wildcard Expression	Common name in an SSL certificate converted into a wildcard expression	String: Common name to convert
SSL.Client.Certificate.Serial	String	Serial of a client certificate	
SSL.ClientContext.IsApplied	Boolean	If true, parameters for setting the client context in SSL-secured communication have been configured.	
SSL.Server.Certificate. AlternativeCNs	List of Wildcard Expression	List of alternative common names for a web server as used in SSL certificates	
SSL.Server.Certificate.CN	String	Common name of a web server provided in a certificate for SSL-secured communication	
SSL.Server.Certificate.CN. HasWildcards	Boolean	If true, the common name for a web server in an SSL certificate includes wildcards.	
SSL.Server.Certificate. DaysExpired	Number	Number of days that an SSL certificate for a web server has expired	
SSL.Server.Certificate. HostAndCertificate	HostAnd Certificate	Host name and certificate for a web server in SSL-secured communication	

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
SSL.Server.Certificate. SelfSigned	Boolean	If true, an SSL certificate for a web server is self-signed.	
SSL.Server.Certificate. SHA1Digest	String	String representing an SHA1Digest of a SSL certificate for a web server	
SSL.Server.CertificateChain. AllRevocationStatusesKnown	Boolean	If true, it is known of all SSL certificates in a certificate chain for a web server whether they are revoked or not.	
SSL.Server.CertificateChain. ContainsExpiredCA	Boolean	If true, an SSL certificate in a certificate chain for a web server has expired.	
SSL.Server.CertificateChain. ContainsRevoked	Boolean	If true, an SSL certificate in a certificate chain for a web server has been revoked.	
SSL.Server.CertificateChain. FirstKnownCAIsTrusted	Boolean	If true, a the certificate authority for issuing SSL certificates that has been found first in a certificate chain for a web server is trusted.	
SSL.Server.CertificateChain. FoundKnownCA	Boolean	If true, a known certificate authority for issuing SSL certificates has been found in a certificate chain for a web server.	
SSL.Server.CertificateChain. IsComplete	Boolean	If true, the chain of SSL certificates for a web server is complete.	
SSL.Server.CertificateChain. Length	Number	Number of SSL certificates in a certificate chain for a web server	
SSL.Server.CertificateChain. PathLengthExceeded	Boolean	If true, the chain of SSL certificates for a web server exceeds the allowed length.	
SSL.Server.Handshake. IsRequested	Boolean	If true, a handshake is requested for setting up a connection to a web server in SSL-secured communication.	
Statistics.Counter.Get	Number	Number of occurrences of an activity or situation recorded on a counter	String: Name of counter
Statistics.Counter.GetCurrent	Number	Number of occurrences of an activity or situation recorded on a counter (fully completed) during the last minute	String: Name of counter
Stopwatch.GetMacroSeconds	Number	Time measured for rule set processing in milliseconds	String: Name of rule set
Stopwatch.GetMilliSeconds	Number	Time measured for rule set processing in macroseconds	String: Name of rule set
StreamDetector.IsMediaStream	Boolean	If true, a requested web object is streaming media. This is the basic property used in streaming media filtering.	
StreamDetector.MatchedRule	String	Name of a streaming media filtering rule that has matched This property is given a value if the *StreamDetector.IsMediaStream* property is set to *true*.	

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
StreamDetector.Probability	Number	Probability for a web object that it is streaming media Values range from 1 to 100. This property is given a value if the *StreamDetector.IsMediaStream* property is set to *true*.	
String.BackwardFind	Number	Position where a substring begins that is found in a string by a backward search Returns -1 if the substring is not found.	1 String: String containing substring 2 String: Substring 3 Number: Position where backward search for substring begins
String.Base64Decode	String	Decoded format of a string specified in base-64 encoded format	String: String in encoded format
String.Base64Encode	String	Base-64 encoded format of a specified string	String: String to encode
String.Concat	String	Concatenation of two specified strings	1 String: First string to concatenate 2 String: Second string to concatenate
String.CRLF	String	Carriage-return line-feed	
String.Find	Number	Position where a substring begins that is found in a string by a forward search Returns -1 if the substring is not found.	1 String: String containing substring 2 String: Substring 3 Number: Position where forward search for substring begins

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
String.FindFirstOf	Number	Position of the first character of a substring found in a string Returns -1 if the substring is not found.	1 String: String containing substring 2 String: Substring 3 Number: Position where search for substring begins
String.FindLastOf	Number	Position of the last character of a substring found in a string Returns -1 if the substring is not found.	1 String: String containing substring 2 String: Substring 3 Number: Position where search for substring begins
String.GetWordCount	Number	Number of words in a string	String: String to get number of words for
String.IsEmpty	Boolean	If true, the specified string is empty.	String: String checked for being empty
String.Length	Number	Number of characters in a string	String: String to count characters for
String.LF	String	Line-feed	
String.MatchWildcard	List of String	List of terms in a string that match a wildcard expression	1 String: String with matching terms 2 Wildcard Expression: Wildcard expression to match 3 Number: Position where search for substring begins

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
String.Replace	String	String having a substring replaced by a string as specified	1 String: String containing substring to replace 2 Number: Position where replacement begins 3 Number: Number of characters to replace 4 String: Replacing string
String.ReplaceAll	String	String having each occurrence of a substring replaced by string as specified	1 String: String containing substring to replace 2 String: Replacing substring 3 String: Substring to replace
String.ReplaceAllMatches	String	String having each occurrence of a substring that matches a wildcard expression replaced by a string as specified	1 String: String containing substring to replace 2 Wildcard Expression: Wildcard expression to match 3 String: Substring to replace

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
String.ReplaceFirst	String	String having first occurrence of a substring replaced by a string as specified	1 String: String containing substring to replace 2 String: Replacing string 3 String: Replacing string
String.ReplaceFirstMatch	String	String having first occurrence of a substring that matches a wildcard expression replaced by a string as specified	1 String: String containing substring to replace 2 Wildcard Expression: Wildcard expression to match 3 String: Replacing substring
String.ReplaceIfEquals	String	String having every occurrence of a substring replaced by a string as specified	1 String: String containing substring to replace 2 String: Substring to replace 3 String: Replacing string

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
String.SubString	String	Substring contained in a string specified by start position and length	1 String: String containing substring 2 Number: Position where substring begins 3 Number: Number of characters in substring If no number is specified, the substring extends to the end of the original
String.SubStringBetween	String	Substring of string extending between two other substrings of this string The search for this substring begins with looking for the first of the other substrings. If this string is found, the search is continued with looking for the second substring. If the first substring is not found, the search has no result. If the second substring is not found, the wanted substring extends from the end of the first substring to the end of the main string.	1 String: String containing substrings 2 String: Substring ending immediately before the wanted substring 3 String: Substring beginning immediately after the wanted substring
String.ToCategory	Category	String converted into a category	String: String to convert
String.ToDimension	Dimension	String converted into a dimension	String: String to convert
String.ToHex	Hex	String converted into a hex value	String: String to convert
String.ToIP	IP	String converted into an IP address	String: String to convert
String.ToIPRange	PRange	String converted into a range of IP addresses	String: String to convert
String.ToMediaType	MediaType	String converted into a media type	String: String to convert

Table A-20 List of properties – S *(continued)*

Name	Type	Description	Parameters
String.ToNumber	Number	String converted into a number	String: String to convert
String.ToStringList	List of String	String converted into a string list The string list is a list of the elements in the string to convert. For example, the string to convert can be a text and the string list a list of the words in this text. The delimiter is a substring that separates elements in the string to convert. For example, in a normal text, the delimiter is the whitespace. The substring can be a single character, such as the whitespace, or multiple characters. To specify the whitespace, hit the space bar. A trim character is a character that appears at the beginning or end of an element in the string to convert, but not in the string list. A trim character can, for example, be a comma, a period, or a single quotation mark. It can also be an "invisible" character, such as a tab stop or a line feed. To specify trim characters, type them in the input field that is provided on the user interface without separating them from each other. Use the following combinations to type invisible characters: \t – tab stop \r – carriage return \n – line feed \b – backspace \\ – backslash If you specify a character as a delimiter, it is also deleted from the resulting string list, so you need not specify it as a trim character.	1 String: String to convert 2 String: Delimiter 3 String: Substring beginning immediately after the wanted substring
String.ToWildcard	Wildcard Expression	String converted into a wildcard expression	String: String to convert
String.URLDecode	String	Standard format of a URL that was specified in encoded format	String: URL in encoded format
String.URLEncode	String	Encoded format of a URL	String: URL to encode
System.HostName	String	Host name of an appliance	
System.UUID	String	UUID (Universal Unique Identifier) of an appliance	

Table A-21 List of properties – T

Name	Type	Description	Parameters
Timer. FirstReceivedFirstSentClient	Number	Processing time consumed between receiving the first byte from a client on the appliance and sending the first byte to this client within a transaction Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.	
Timer. FirstSentFirstReceivedServer	Number	Processing time consumed between sending the first byte from the appliance to a web server and receiving the first byte from this server within a transaction Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.	
Timer.HandleConnectToServer	Number	Processing time consumed for connecting to a web server within a transaction	
Timer. LastReceivedLastSentClient	Number	Processing time consumed between receiving the last byte from a client on the appliance and sending the last byte to this client within a transaction Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.	
Timer.LastSentLastReceived FromServer	Number	Processing time comsumed between sending the last byte from the appliance to a web server and receiving the last byte from this server within a transaction Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.	
Timer. ResolveHostNameViaDNS	Number	Processing time consumed for looking up a host name on a DNS server within a transaction Only lookups on external servers are considered. Cache lookups are disregarded.	
Timer. TimeConsumedByRuleEngine	Number	Time consumed by the rule engine to process a request throughout all relevant processing cycles Processing a request through all relevant processing cycles is considered one transaction.	
Timer.TimeForTransaction	Number	Time consumed by the rule engine to process a request that has been received on the appliance through all relevant processing cycles This property is only supported for HTTP or HTTPS connections, not FTP connections.	
Tunnel.Enabled	Boolean	If true, an HTTP or HTTPS tunnel is enabled	

Table A-22 List of properties – U

Name	Type	Description	Parameters
URL	String	URL of a web object	
URL.Categories	List of Category	List of URL categories that a URL belongs to	
URL.CategoriesForURL	List of Category	List of URL categories that a specified URL belongs to	String: URL in string format
URL.DestinationIP	IP	IP address for a URL as found in a DNS lookup	

Table A-22 List of properties – U *(continued)*

Name	Type	Description	Parameters
URL.Host.BelongsToDomains	Boolean	If true, a host that access was requested to by submitting a particular URL belongs to one of the domains in a list. The list is specified as the property parameter. You can use this property to match anything to the domain name in a URL or anything to the left of a dot of a domain name (*.domain.com). Terms including the domain name (*domain.com) are not counted as matches. *Example:* *Domain List* is the string list specified as the property parameter. It contains the following entries (dots preceding a domain name in a URL are omitted): *twitter.com* *mcafee.com* *dell.com* *k12.ga.us* *xxx* Then the criteria: *URL.Host.BelongsToDomains("Domain List") equals true* matches for the following URLs: *http://twitter.com* *http://www.twitter.com* *http://my.mcafee.com* *http://my.support.dell.com* *http://www.dekalb.k12.ga.us* *any.site.xxx* but not for: *http://maliciouostwitter.com* *http://www.mymcafee.com* *http://www.treasury,ga.us* Using this property avoids the effort of creating more complicated solutions to accomplish the same, for example: • Using two entries in a list of wildcard expressions, such as: *twitter.com* and **twitter.com* • Using a single, complex entry in a list of wildcard expressions, such as: *regex((.*\.|.?)twitter\.com)*	List of string: List of domains

Table A-22 List of properties – U *(continued)*

Name	Type	Description	Parameters
		If these entries were contained in the list *Other Domain List*, the following criteria would match for the *twitter.com* domain: *URL.Host matches in list "Other Domain List"*	
URL.FileName	String	Name of a file that can be accessed through a URL	
URL.FileExtension	String	Extension of the file name for a requested file	
URL.Geolocation	String	ISO 3166 code for the country where the host that a URL belongs to is located If a value is to be assigned to this property, the following option of the settings for the URL Filter module must be enabled: *Only use online GTI web reputation and categorization services.*	
URL.GetParameter	String	Parameter of a URL in string format	String: Parameter name
URL.HasParameter	Boolean	If true, a specified parameter belongs to the parameters of a URL.	String: Parameter name
URL.Host	String	Host that a URL belongs to	
URL.HostIsIP	Boolean	If true, the URL that is submitted for access to a host is an IP address.	
URL.IsHighRisk	Boolean	If true, the reputation score of a URL falls in the high risk range.	
URL.IsMediumRisk	Boolean	If true, the reputation score of a URL falls in the medium risk range.	
URL.IsMinimalRisk	Boolean	If true, the reputation score of a URL falls in the minimal risk range.	
URL.IsUnverifiedRisk	Boolean	If true, the reputation score of a URL falls in the unverified risk range.	
URL.Parameters	List of String	List of URL parameters	
URL.ParametersString	String	String containing the parameters of a URL If the URL has parameters, the string begins with the ? character.	
URL.Path	String	Path name for a URL	
URL.Port	Number	Number of a port for a URL	
URL.Protocol	String	Protocol for a URL	

Table A-22 List of properties – U *(continued)*

Name	Type	Description	Parameters
URL.Raw	String	URL in the format originally received on the appliance from a client or other instances of the network. Using this property for rule configuration will speed up processing because it saves the time used for converting URL code to a human readable format, as it is done for the simple *URL* property.	
URL.Reputation	Number	Reputation score for a URL	
URL.ReputationForURL	Number	Reputation score for a specified URL	String: URL in string format
URL.ReputationString	String	String representing reputation score fora URL	
User-Defined.cacheMessage	String	Message text providing information on web cache usage	
User-Defined.eventMessage	String	Message text providing information on an event	
User-Defined.loadMessage	String	Message text providing information on CPU overload	
User-Defined.logLine	String	Entry written into a log file	
User-Defined. monitorLogMessage	String	Entry written into a log file	
User-Defined. notificationMessage	String	Text of a notification message	
User-Defined. requestLoadMessage	String	Message text providing information on request overload	
User-Defined. requestsPerSecond	Number	Number of requests processed on an appliance per second	

Table A-23 List of properties – W

Name	Type	Description	Parameters
Wildcard.ToString	String	Wildcard expression converted into a string	Wildcard Expression: Wildcard expression to convert

Wildcard expressions

When completing configuration activities on an appliance, you can use wildcard expressions for several purposes, for example, to match URLs on blocking lists and whitelists.

There are two types of wildcard expressions you can use:

- **Glob expressions** — Using these is the default.

  More information about this type of expressions is, for example, provided on the following Linux man page:

  glob(7)

- **Regular expressions (Regex)** — If you want to use these, you need to type the term *regex* first and then include the regular expression in parentheses, for example:

  ```
  regex(a*b)
  ```

  The regular expressions that are used on the McAfee Web Gateway appliance follow the Perl Regular Expression syntax. Information on this syntax is, for example, provided on the following Linux man page:

  perlre(1)

See also
List of important special glob characters on page 443
List of important special regex characters on page 444

Test a wildcard expression

When adding a wildcard expression to a list, you can test it before actually adding it.

Task

1. Select **Policy | Lists**.
2. On the lists tree, expand **Wildcard Expressions** and select a list.
3. Click the **Add** icon on the settings pane.

   The **Add Wildcard Expression** window opens.
4. Type a wildcard expression in the input field, then click **Test**.

   The **Wildcard Expression Test** window opens to display information on whether the expression is valid.

List of important special glob characters

The following table provides a list of important special characters you can use to create *glob* type wildcard expressions.

Table A-24 List of important special glob characters

Character	Description

?	Matches any single character (if not between square brackets).
	For example, `?est` matches:
	`best`
	`rest`
	`test`
	and others

*	Matches any string, including the empty string (if not between square brackets).
	For example, `b*` matches:
	`b`
	`best`
	`binary`
	and others

[...]	Matches any of the single characters included in the square brackets.
	? and * are normal characters between square brackets.
	For example, `[a5?]` matches:
	`a`
	`5`
	`?`
	The first character must not be an ! (exclamation mark).

!	Matches any single character except those following the exclamation mark.
	For example, `[!ab]` matches:
	`c`
	`S`
	`%`
	but not:
	`a`
	`b`

-	Is used to denote a range of characters.
	For example, `[a-f A-F 0-5]` matches:
	`d`
	`F`
	`3`
	and others

Table A-24 List of important special glob characters *(continued)*

Character	Description

/	Is not matched by ? or * and cannot be included in [...] or be part of a range.
	This means, for example, that
	`http://linux.die.net/*`
	does not match the following pathname:
	`http://linux.die.net/man/7/glob`
	The pathname is, however, matched by:
	`http://linux.die.net/*/*/*`

\	If preceding ?, *, or [, these are normal characters.
	For example, `[mn\*\[]` matches:
	`m`
	`n`
	`*`
	`[`

.	A . (dot) at the beginning of a file name must be matched explicitly.
	For example, the command:
	`rm *`
	will not remove the file *.profile*.
	However, the following command will:
	`rm .*`

List of important special regex characters

The following table provides a list of important special characters you can use to create*regex* type wildcard expressions.

The examples given here include the term *regex* and parentheses. You need to use both when working with these expressions on an appliance.

Table A-25 List of important special regex characters

Character	Description

.	Matches any single character.
	For example, `regex(.est)` matches:
	`best`
	`rest`
	`test`
	and others

*	Matches the preceding character zero or more times
	For example, `regex(a*b)` matches:
	`b`
	`ab`
	`aaaaab`
	and others

+	Matches the preceding character once or more times.
	For example, `regex(c+d)` matches:
	`cd`
	`ccccd`
	and others

?	Matches the preceding character zero times or once.
	For example, `regex(m?n)` matches:
	`n`
	`mn`

^	Matches the beginning of a line
$	Matches the end of a line

Table A-25 List of important special regex characters *(continued)*

Character	Description

{...}	Are used to match a character as many times as specified.
	Options:
	• *a{n}* — Matches a character *n* times
	For example, `regex(a{3})` matches:
	`aaa`
	• *a{n,}* — Matches a character *n* and more times
	For example, `regex(p{4,})` matches:
	`pppp`
	`ppppp`
	and others
	• *a{n,m}* — Matches between *n* and *m* times, including the limiting values
	For example, `regex(q{1,3})` matches:
	`q`
	`qq`
	`qqq`

|	Separates expressions that match alternatively.
	For example, `regex(abc|klm)` matches:
	`abc`
	`klm`

(...)	Delimits an alternative expression combined with another expression.
	For example, `regex(bi(n|rd))` matches:
	`bin`
	`bird`

[...]	Matches any of the single characters included in the square brackets.
	For example, `regex([bc3])` matches:
	`b`
	`c`
	`3`

-	Is used to denote a range of characters in a bracketed expression.
	For example, `regex([c-f C-F 3-5])` matches:
	`d`
	`F`
	`4`
	and others

Table A-25 List of important special regex characters *(continued)*

Character	Description

^	Matches any single character in a bracketed expression except those following the accent circonflexe.
	For example, `regex([^a-d])` matches:
	`e`
	`7`
	`&`
	and others, but not
	`a`
	`b`
	`c`
	`d`

\	If preceding a special character, turns it into a normal character.
	For example, `regex(mn\+)` matches:
	`mn+`
	If preceding some normal characters, matches a particular class of characters.
	For information on these classes, refer to the *perlre* man page or other documentation. The following are examples of frequently used character classes.
	`regex(\d)` matches numerical characters (digits), such as:
	`3`
	`4`
	`7`
	and others
	`regex(\w)` matches alphabetical characters, such as:
	`a`
	`F`
	`s`
	and others
	`regex(\D)` matches all characters that are not digits, such as:
	`c`
	`T`
	`%`
	and others

B Third-party software

The following lists provide information on third-party software used in developing the McAfee Web Gateway appliance software.

Information is presented in alphabetical order based on the third-party software names.

Third-party software used in developing the user interface of the appliance software is listed in a separate list following the main list.

Contents

Main list

The following list provides information on third-party software used in developing the McAfee Web Gateway appliance software, except for the third-party software that was used to develop the user interface.

Information is provided in alphabetical order based on the third-party software names.

Arabica C++ XML Library

Made available under a license that is an adaptation of a Berkeley Software Distribution (BSD) license.

Copyright © 2001-2010 Jez UK Ltd. All rights reserved.

ASN.1 Compiler

Made available under a Berkeley Software Distribution (BSD) license.

Copyright © 2003-2010 Lev Walkin.

Boost C++ Libraries

Made available under the Boost Software License, version 1.0.

Copyright © 1998-2005 Bernan Dawes, David Abrahams.

Copyright © 2004-2007 Rene Rivera.

bzip2

Made available under a license that is an adaptation of a Berkeley Software Distribution (BSD) license.

Copyright © 1996-2007 Julian Seward.

libcurl

Made available under a license that is an adaptation of an MIT/X license.

Copyright © 1996-2011 Daniel Stenberg. All rights reserved.

libiconv

Made available under the GNU Lesser General Public License (LGPL), version 2.1.

Copyright © 1998, 2010 Free Software Foundation, Inc.

libxml2

Made available under the MIT License.

LZMA SDK

The LZMA SDK is placed in the public domain.

OpenLDAP

Made available under the OpenLDAP Public License, version 2.8.

Copyright © 2012 OpenLDAP Foundation.

OpenSSL

Made available under a license that is an adaptation of an Apache License (APL).

Copyright © 1999-2009 The OpenSSL Project. All rights reserved.

RapidXml Library

Made available under the Boost Software License, version 1.0, or the MIT License.

Copyright © 2006, 2009 Marcin Kalicinski.

SOCI C++ Database Access Library

Made available under the Boost Software License, version 1.0.

Copyright © 2004-2006 Maciej Sobczak, Stephen Hutton.

UDNS: DNS Resolver Library

Made available under a GNU Lesser General Public License (LGPL).

UnRAR

Made available under a license that is an adaptation of a Berkeley Software Distribution (BSD) license.

Unzip

Made available under a license that is an adaptation of a Berkeley Software Distribution (BSD) license.

Copyright © 1990-2009 Info-ZIP. All rights reserved.

Info-ZIP is a set of individuals including Mark Adler, John Bush, and others.

zlib

Made available under a license that is an adaptation of a Berkeley Software Distribution (BSD) license.

Copyright © 1995-2012 Jean-loup Gailly and Mark Adler.

User interface list

The following list provides information on third-party software used in developing the user interface of the McAfee Web Gateway appliance software.

Information is provided in alphabetical order based on the third-party software names.

Apache Abdera

Made available under the Apache License (APL), version 2.0.

Copyright © 2006-2010 The Apache Software Foundation.

Apache Axiom

Made available under the Apache License (APL), version 2.0.

Copyright © 2004-2012 The Apache Software Foundation. All rights reserved.

Apache Commons

Made available under the Apache License (APL), version 2.0.

Copyright © 2012 The Apache Software Foundation. All rights reserved.

Apache Commons Codec

Made available under the Apache License (APL), version 2.0.

Copyright © 2002-2011 The Apache Software Foundation. All rights reserved.

Apache Commons Logging

Made available under the Apache License (APL), version 2.0.

Copyright © 2001-2008 The Apache Software Foundation..

Apache log4j

Made available under the Apache License (APL), version 2.0.

Copyright © 2011 The Apache Software Foundation.

Apache Tomcat

Made available under the Apache License (APL), version 2.0.

Copyright © 1999-2012 The Apache Software Foundation.

ASM

Made available under a project license of the OW2 consortium.

Copyright © 1999-2009 OW2 Consortium.

Fugue Icons

Made available under the Creative Commons Attribution License, version 3.0.

Glazedlists

Made available under the GNU Lesser General Public License (LGPL), version 2.1, or the Mozilla Public License (MPL), version 1.1.

Copyright © 2011 Oracle and/or its affiliates. All rights reserved.

Jakarta Commons HttpClient

Made available under the Apache License (APL), version 2.0.

Copyright © 2001-2011 Apache Software Foundation.

Jakarta ORO

Made available under the Apache License (APL), version 2.0.

Copyright © 1999-2004 The Apache Software Foundation.

Jaxen XPath Library

Made available under a project license of Codehaus.

Copyright © 2001-2010 Codehaus.

JCommon

Made available under the GNU Lesser General Public License (LGPL), version 2.1 or later.

Copyright © 2007-2011 Object Refinery Limited.

Jersey

Made available under the Common Development and Distribution License (CDDL), version 1.1, or GNU General Public License (GPL), version 2, with classpath exception.

Copyright © 2008-2012 Oracle and/or its affiliates. All rights reserved.

JGoodies UIForms Lite

Made available under a Berkeley Software Distribution (BSD) license.

Copyright © 2012 JGoodies.

JFree Chart

Made available under the GNU Lesser General Public License (LGPL), version 2.1.

Copyright © 2005-2011 Object Refinery Limited.

Jide Common

Made available under the GNU General Public License (GPL), version 2, with classpath exception, or a free commercial license.

The GPL is the license under which the Java platform is made available. The free commercial license is the same as the license under which all other Jide products are made available, differing from it only in that it is free of charge.

Copyright © 2011 Oracle and/or its affiliates. All rights reserved.

JSR-000154 Java Servlet 2.5

Made available under the Apache License (APL), version 2.0.

Copyright © 2011 Oracle Corporation and/or its affiliates.

JSR-000311 Java API for RESTful Web Services

Made available under the Common Development and Distribution License (CDDL), version 1.1, or the GNU General Public License (GPL), version 2, with classpath exception.

Copyright © 2011 Oracle Corporation and/or its affiliates.

New Java Plug-in

Made available under the license agreement that accompanies the distribution of the Java software.

Copyright © 2008-2012 Oracle and/or its affiliates. All rights reserved.

opencsv

Made available under the Apache License (APL), version 2.0.

Rhino: JavaScript for Java

Made available in most parts under the Mozilla Public License (MPL), version 1.1, or the GNU General Public License (GPL), version 2.

Silk Icons

Made available under the Creative Commons Attribution License, version 2.5 or 3.0.

StAX2 and Woodstox

Made available under the Apache License (APL) , version 2.0, or the GNU Lesser General Public License (LGPL), version 2.1.

The Legion of the Bouncy Castle

Made available under the license that is provided by The Legion of the Bouncy Castle, which is an adaptation of a MIT X11 license.

Copyright © 2000-2011 The Legion of the Bouncy Castle.

Trove

Made available under the GNU Lesser General Public License (LGPL), version 2.1.

Two classes (HashFunctions and PrimeFinder) included in Trove are made available under a license of the European Organization for Nuclear Research (CERN).

XStream

Made available under a Berkeley Software Distribution (BSD) license.

Index