Product Guide

McAfee Web Gateway 7.8.0
## Contents

1 **Overview of Web Gateway**  
   Key features of Web Gateway ...................................................... 13  
   How Web Gateway works .......................................................... 14  

2 **User interface**  
   Discarding changes ....................................................................... 17  
   Discard changes by reloading data .................................................. 17  
   Administering Web Gateway without the user interface ....................... 17  

3 **System configuration**  
   Initial system settings .................................................................... 20  
   System settings ................................................................................ 20  
   System settings overview .................................................................. 21  
   Network interface bonding .............................................................. 22  
   Configure network interface bonding .............................................. 22  
   Checking the bonding configuration .................................................. 24  
   Source-based routing ....................................................................... 25  
   Configure source-based routing for a management network interface .... 25  
   Cache volume resizing ..................................................................... 27  
   System files ...................................................................................... 27  
   Update handling ............................................................................... 28  
   Update database information manually .......................................... 28  
   Schedule automatic engine updates .................................................. 29  
   Closed network updates .................................................................. 29  
   Update an appliance in a closed network .......................................... 30  

4 **Proxies**  
   Configure proxies ............................................................................ 31  
   Explicit proxy mode ........................................................................ 32  
   Configure the explicit proxy mode .................................................... 33  
   Best practices - Configuring the Proxy HA mode ............................... 33  
   Configure the Proxy HA mode .......................................................... 34  
   Resolving issues with a Proxy HA configuration ............................... 36  
   Best practices - High Availability configuration size limits .................... 36  
   Best practices - Configuring the explicit proxy mode with WCCP ............ 38  
   Configure use of the WCCP protocol ............................................... 39  
   Settings for a WCCP service ............................................................ 40  
   Troubleshooting WCCP-related issues .............................................. 41  
   Transparent router mode .................................................................. 42  
   Configure the transparent router mode .............................................. 43  
   Configure nodes in transparent router mode ...................................... 43  
   Transparent bridge mode .................................................................. 46  
   Configure the transparent bridge mode .............................................. 47  
   Configure nodes in transparent bridge mode ...................................... 47  
   Best practices - Fine-tuning a transparent bridge configuration .............. 50
Create a tenant ID .................................. 106
Add a scheduled job .................................. 106
Update the appliance software in a Central Management configuration .......................... 107

6 Policy configuration .................................. 109
Configuring a web security policy .................................. 110
Fields of web security and rule sets .................................. 111
Fields of web security covered by default rule sets .................................. 111
Fields of web security covered by library rule sets .................................. 112
Access a rule set .................................. 112
Rule sets .................................. 112
Rule set system .................................. 113
Rule set library .................................. 114
Rule set views .................................. 115
Filtering process .................................. 120
Filtering cycles .................................. 121
Process flow .................................. 122
Common tasks in policy configuration .................................. 123
Configuring a rule element .................................. 123
Enabling a rule set for cloud use .................................. 125

7 Complete rules .................................. 127
Rule elements .................................. 127
Rule format on the user interface .................................. 128
Rule representation in the documentation text .................................. 129
Create a rule .................................. 131
Name and enable a rule .................................. 132
Add the rule criteria .................................. 132
Add the rule action .................................. 133
Add a rule event .................................. 134
Create a rule set .................................. 135
Import a rule set .................................. 136
Restrict access to a rule set .................................. 137

8 Lists .................................. 139
List types .................................. 140
Access a list .................................. 141
Access a list on the Lists tab .................................. 141
Access a list in a rule .................................. 141
Create a list .................................. 142
Add a new list .................................. 142
Fill a list with entries .................................. 142
Work with different types of lists .................................. 143
Add a wildcard expression to a global whitelist for URLs .................................. 143
Add a URL category to a blocking list .................................. 144
Add a media type to a media type filter list .................................. 144
External lists .................................. 145
Use of external list data in rules .................................. 146
Substitution and placeholders .................................. 147
Configure the External Lists module .................................. 147
Configure general settings for external lists .................................. 148
Subscribed lists .................................. 148
Create a subscribed list .................................. 149
Updating subscribed lists .................................. 150
Creating a content file for a customer-maintained list .................................. 150
Best practice: Working with a McAfee-supplied subscribed list .................................. 152
Contents

Map Type lists ................................... 154
  Create a Map Type list ........................................ 154
  Using properties to work with Map Type lists .............. 155
  Retrieving map data from external and subscribed lists ... 156

Common Catalog .................................. 157
  Prepare the use of Common Catalog lists .................... 157
  Set up a user account for Common Catalog lists .......... 158
  Set up an administrator account for Common Catalog lists ... 158
  Enable use of the REST interface for Common Catalog lists ... 159
  Sample settings for registering Web Gateway on a McAfee ePO server ... 159

JavaScript Object Notation data ............................. 159

9 Settings 165
  Types of settings ........................................... 165
  Access settings .............................................. 166
    Access action and module settings on the Settings tab ...... 166
    Access action and module settings in a rule ............ 167
    Access system settings ................................... 167
  Create action and module settings ........................... 167

10 Web filtering 169
  Anti-malware filtering ...................................... 169
  Anti-malware filtering process ............................. 169
  Gateway Anti-Malware rule set ................................ 171
  Change the module combination for scanning web objects ... 172
  Using URL information for anti-malware filtering .......... 173
  Integrating TIE server information with anti-malware filtering ...... 174
  Dealing with a missing host header ........................ 179
  Media stream scanning .................................... 182
  Anti-malware queue ...................................... 182
  URL filtering ............................................. 183
    Configure key elements for URL filtering ............... 185
    Configure URL filtering using the complete rules view ... 185
    Configure settings for the URL Filter module .......... 185
    Best practices - Using URL properties to whitelist web objects ... 186
    URL Filtering rule set ................................... 191
    URL filtering using the Dynamic Content Classifier .... 193
    Using your own URL filter database .................. 194
    URL filtering using an IFP proxy ....................... 195
  Media type filtering .................................... 198
    Configure key elements for media type filtering ...... 199
    Configure media type filtering using the complete rules view ... 200
    Modify a media type filtering rule ..................... 200
    Media Type Filtering rule set .......................... 201
  Application filtering .................................... 202
    Configure application filtering ....................... 204
    Create a list for application filtering ............... 205
    Modify the risk level in an application filtering rule ... 206
    Application Control rule set .......................... 206
  Streaming media filtering ............................... 208
    Configure streaming media filtering .................. 209
    Configure the streaming media detection module ....... 210
    Best practices - Configuring the Stream Detector ...... 210
  Global whitelisting ..................................... 212
    Configure global whitelisting .......................... 212
    Global Whitelist rule set ............................. 213
| SSL scanning | 214 |
| Configure SSL scanning | 215 |
| Configure the modules for SSL scanning | 216 |
| Replace the default root certificate authority | 217 |
| Client certificate list | 218 |
| Using AIA entries for certificate downloads | 220 |
| Sending tapped SSL traffic to a monitoring device | 220 |
| SSL Scanner rule set | 221 |

| Hardware Security Module | 226 |
| Using a Hardware Security Module | 226 |
| Key handling with a Hardware Security Module | 227 |
| Work with a Hardware Security Module | 228 |

| Advanced Threat Defense | 232 |
| Workflows for using Advanced Threat Defense | 234 |
| Criteria for additional scanning by Advanced Threat Defense | 235 |
| Configuration elements for using Advanced Threat Defense | 235 |
| Using an existing Advanced Threat Defense scanning report | 237 |
| Using an ongoing Advanced Threat Defense scanning run | 238 |
| Limiting object sizes for scanning by Advanced Threat Defense | 239 |
| Configure the use of Advanced Threat Defense | 240 |
| Configure key elements for using Advanced Threat Defense | 242 |
| Configure settings for using Advanced Threat Defense | 242 |
| Monitoring the use of Advanced Threat Defense | 242 |
| McAfee Advanced Threat Defense rule set | 244 |
| ATD - Offline Scanning with Immediate File Availability rule set | 245 |

| Data loss prevention | 247 |
| Configure data loss prevention | 250 |
| Configure data loss prevention using default classifications | 251 |
| Configure data loss prevention using dictionary entries | 251 |
| Data Loss Prevention rule set | 253 |
| Preventing data loss using an ICAP server | 254 |

| Using an on-premise DLP server from the cloud | 256 |
| Configure the use of an on-premise DLP server from the cloud | 257 |

11 Authentication

| Authentication | 259 |
| Authenticating users | 260 |
| Configure authentication | 261 |
| Configure the Authentication module | 261 |
| Implement a different authentication method | 262 |
| Using system settings to configure authentication | 262 |
| Join the appliance to a Windows domain | 263 |
| NTLM Agent authentication | 263 |
| Configure NTLM Agent authentication | 264 |
| LDAP digest authentication | 264 |
| Best practices - Configuring authentication for deployment types | 266 |
| Authentication for the explicit proxy mode | 267 |
| Authentication for transparent modes | 269 |
| Authentication for the explicit proxy mode with WCCP | 272 |
| Best practices - Configuring LDAP authentication | 273 |
| Configure the LDAP method for authenticating a user | 274 |
| Configure the settings for the LDAP authentication method | 275 |
| Configure queries for user and group attributes | 276 |
| Storing an attribute in a separate property | 277 |
| Storing the original user name for logging | 277 |
| Testing and troubleshooting LDAP authentication | 279 |
| Instant messaging authentication | 281 |
Configure instant messaging authentication ................................................. 282
Configure the Authentication module for instant messaging authentication .......... 282
Configure the File System Logging module for instant messaging authentication .... 283
IM Authentication rule set ........................................................................... 283
One-time passwords ...................................................................................... 285
Configure one-time passwords for authenticating users ................................. 286
Configure one-time passwords for authorized overriding ................................ 286
Configure the settings for one-time passwords .............................................. 287
Authentication Server (Time/IP Based Session with OTP) rule set ....................... 288
Authorized Override with OTP rule set ....................................................... 290
Authentication Server (Time/IP Based Session with OTP and Pledge) rule set ......... 292
Authorized Override with OTP and Pledge rule set ...................................... 294
Client Certificate authentication .................................................................... 296
Use of certificates for Client Certificate authentication ..................................... 296
Rule sets for Client Certificate authentication .............................................. 297
Redirecting requests to an authentication server ........................................... 298
Implement Client Certificate authentication .................................................. 299
Import the Authentication Server (for X509 Authentication) rule set ................... 300
Modify a rule set to configure the use of server certificates ............................... 300
Modify a rule set to configure the use of certificate authorities ............................ 301
Configure a listener port for incoming requests on the appliance ......................... 302
Import the Cookie Authentication (for X509 Authentication) rule set .................. 303
Modify a rule set to change the listener port for incoming requests ........................ 303
Import a client certificate into a browser ........................................................ 304
Administrator accounts ............................................................................... 306
Add an administrator account ....................................................................... 306
Edit an administrator account ..................................................................... 306
Delete an administrator account ................................................................... 306
Manage administrator roles ......................................................................... 307
Configure external account management ..................................................... 307

12 Quota management .................................................................................. 309
Imposing quotas and other restrictions on web usage ....................................... 309
Time quota ................................................................................................. 312
Configure time quotas ................................................................................. 312
Time Quota rule set ..................................................................................... 313
Volume quota .............................................................................................. 314
Configure volume quotas ............................................................................ 315
Volume Quota rule set ................................................................................ 315
Coaching ....................................................................................................... 318
Configure coaching ....................................................................................... 318
Coaching rule set ......................................................................................... 319
Authorized override ..................................................................................... 320
Configure authorized overriding .................................................................... 321
Authorized Override rule set ....................................................................... 321
Blocking sessions ........................................................................................ 323
Configure blocking sessions ......................................................................... 323
Blocking Sessions rule set ........................................................................... 323

13 User messages ......................................................................................... 325
Sending messages to users ........................................................................... 325
Edit the text of a user message ..................................................................... 327
Modifying a block page ................................................................................ 327
Modifying the parts of a block page ................................................................ 328
Modify the footer of a block page ................................................................. 328
Modify the issue-related part of a block page ................................................ 329
Change the logo on a block page ........................................ 330
Change the color of the background bars on a block page ......... 331

14 Supporting functions .................................................. 333
Functions supporting web filtering ..................................... 333
Web caching .................................................................... 333
Verify the enabling of the web cache .................................. 334
Web Cache rule set .......................................................... 334
Progress indication .......................................................... 336
  Configure progress indication ......................................... 336
  Configure the progress indication modules ....................... 337
  Best practice: Working with progress indication methods .... 338
  Progress Indication rule set ........................................... 342
File opening ................................................................. 342
  File opening process .................................................... 342
  Formats for file opening ............................................. 343
  Enable Opener rule set .................................................. 343
Bandwidth throttling ....................................................... 344
  Basic bandwidth throttling ......................................... 345
  Bandwidth throttling using classes ............................... 347
Next-hop proxies .......................................................... 350
  Next-hop proxy modes .............................................. 350
  Configure next-hop proxies ....................................... 352
  Add a next-hop proxy to a list ..................................... 353
  Configure the Next Hop Proxy module ......................... 353
  Configure next-hop proxy stickiness ......................... 354
  Next-hop proxies for SOCKS traffic ............................ 354
  Best practices - Troubleshooting next-hop proxy issues .... 357
  Next Hop Proxy rule set ............................................. 360

15 Cloud single sign-on .................................................... 361
How cloud single sign-on is configured ............................. 362
Considerations when exporting and importing the SSO rule set . 363
SSO process in proxy and non-proxy modes ......................... 364
Supported authentication methods ................................... 365
SSO Catalog of supported cloud services ........................... 366
  Viewing the SSO Catalog ........................................... 366
  SSO Catalog in the user interface ............................... 367
  SSO Catalog as a service .......................................... 367
  Generic vs. individual connector templates .................... 368
  Configure a custom cloud connector using a template ....... 369
  Delete a custom cloud connector ................................ 369
  Locate information about the latest SSO updates .............. 370
SSO Connector lists ....................................................... 370
  Configuring cloud access through SSO Connector lists ....... 370
  Add a cloud connector to an SSO Connector list ............ 371
Providing SSO services for HTTP cloud applications ............ 371
  The SSO credential model for HTTP cloud applications .... 372
  Configure an HTTP cloud connector ............................ 372
  Configure a generic HTTP cloud connector .................... 372
Providing SSO services for SAML 2.0 cloud applications ....... 373
  How SAML single sign-on is initiated ......................... 373
  Certificate management for SAML single sign-on .......... 375
  Configure a SAML2 cloud connector ............................ 376
  Configure a generic SAML2 cloud connector ................... 377
  Configuring external data sources for SAML single sign-on . 377
### 16 Cloud storage encryption

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypting and decrypting cloud storage data</td>
<td>417</td>
</tr>
<tr>
<td>Configure encryption and decryption of cloud storage data</td>
<td>420</td>
</tr>
<tr>
<td>Configure the settings for encrypting and decrypting data</td>
<td>420</td>
</tr>
<tr>
<td>Decrypt cloud storage data manually</td>
<td>421</td>
</tr>
<tr>
<td>Cloud Storage Encryption rule set</td>
<td>421</td>
</tr>
</tbody>
</table>

### 17 Hybrid solution

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premise and remote web access</td>
<td>423</td>
</tr>
<tr>
<td>Components of the hybrid solution</td>
<td>423</td>
</tr>
<tr>
<td>How the hybrid solution works</td>
<td>424</td>
</tr>
<tr>
<td>Authentication considerations for the hybrid solution</td>
<td>426</td>
</tr>
<tr>
<td>Why some rules are restricted</td>
<td>427</td>
</tr>
<tr>
<td>Managing the hybrid solution</td>
<td>427</td>
</tr>
<tr>
<td>Identifying rule sets not supported in the cloud</td>
<td>428</td>
</tr>
<tr>
<td>Enable rule sets for hybrid synchronization</td>
<td>428</td>
</tr>
<tr>
<td>Configure and enable the hybrid solution</td>
<td>428</td>
</tr>
<tr>
<td>Verify that policy synchronization succeeded</td>
<td>429</td>
</tr>
<tr>
<td>Add hybrid information to a block page</td>
<td>429</td>
</tr>
</tbody>
</table>

### 18 Monitoring

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>431</td>
</tr>
<tr>
<td>Access the dashboard</td>
<td>432</td>
</tr>
<tr>
<td>Alerts tab</td>
<td>432</td>
</tr>
<tr>
<td>Charts and Tables tab</td>
<td>433</td>
</tr>
<tr>
<td>Logging</td>
<td>434</td>
</tr>
</tbody>
</table>
Overview of Web Gateway

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

**Filtering web traffic**

Following the implemented web security rules, Web Gateway 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.

This figure provides an overview of the filtering process.

![Diagram of filtering web traffic](image)

**Figure 1-1 Filtering web traffic**

1 – Your network
2 – Web Gateway
3 – Web

1 – Sends requests to the web.
2 – Filters requests and responses.
3 – Sends responses to your network.

**Filtering on premise and in the cloud**

Web Gateway is part of an integrated solution known as McAfee® Web Protection (Web Protection). This solution provides protection against threats that arise when users of your organization access the web from inside or outside your local network.

Users who access the web from inside your local network are often referred to as on-premise users. Outside access happens when users of your organization work on systems that are not connected to this network, for example, while they travel or work at home. These users are often referred to as cloud users.

McAfee® Web Gateway Cloud Service (McAfee® WGCS) is the part of the solution that protects web usage by cloud users.

As an integrated solution, Web Protection allows you to enforce the same security policy for web access by both on-premise and cloud users.

**Contents**

- Key features of Web Gateway
Key features of Web Gateway

Filtering web traffic is a complex process. The key features of Web Gateway contribute to it in different ways.

Intercepting web traffic

This is a prerequisite for any filtering of web objects or users. It is achieved by the proxy functions of Web Gateway, which can be performed under different network protocols, such as HTTP, HTTPS, HTTP2, FTP, XMPP, and others.

When the proxy functions are configured, the appliance can run in explicit proxy mode or in one of several transparent modes.

Authenticating users

Authentication functions of Web Gateway 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.

Filtering web objects

The anti-malware functions on Web Gateway scan and filter web traffic and block web objects if they are infected.

Other functions filter URLs that users request access to, using information from the McAfee® Global Threat Intelligence™ (McAfee GTI) 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.

Monitoring the filtering process

The monitoring functions of Web Gateway 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 include external components in the monitoring process, such as the McAfee® ePolicy Orchestrator™ Cloud (McAfee® ePO™ Cloud) server or an SNMP agent.
How Web Gateway works

A 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)

![Appliance subsystems and modules](image-url)
Operating system

The subsystems of the appliance rely on the functions of its operating system, which is MLOS 2 (McAfee Linux Operating System, version 2).

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.
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.

Administering Web Gateway without the user interface

An additional interface is provided that allows you to administer Web Gateway without being logged on to its standard user interface. This alternative interface is referred to as REST (Representational State Transfer) interface.

Using the REST interface, you can perform administration activities on a particular Web Gateway appliance and on others that are connected to it, for example, turn off an appliance, restart it, work with lists and settings, or trigger updates.
For an introduction to the REST interface that explains basic methods of working with it and provides sample script lines for communicating with the interface, see the *REST interface* section in the appendix of this guide.
System configuration

The system of a Web Gateway appliance is configured to support the filtering functions that protect your network against threats arising from the web.

When performing this configuration, you will be dealing with several concepts, functions, and processes.

- **Initial system settings** — System configuration is in part performed during the initial setup of Web Gateway.

  Settings that are configured during this setup include the primary network interface, host name, root password, and others.

- **System settings** — After the initial setup you can configure more system settings and also modify the initial settings.

  This includes configuring system settings for:

  - **Network interfaces** — Network interfaces are configured to enable processing of web traffic on a Web Gateway appliance, specifying the host name, gateways, use of the IPv4 or IPv6 protocol, and other settings.

    Some of these settings are already configured during the initial setup.

  - **Proxies** — Web Gateway can be configured to run as a proxy that intercepts web traffic and transmits it if this is allowed by the rules of your web security policy.

    Proxies can be configured in different ways regarding:

    - Network mode, which can be an explicit (also known as direct) proxy mode or a transparent mode
    - Network protocol, which can be, for example, HTTP, HTTPS, FTP, ICAP, or IFP, to enable the filtering of web traffic that is going on under any of these protocols

  - **Cluster nodes** — Instead of running a Web Gateway appliance in a standalone mode, you can run multiple appliances as nodes in a cluster.

    These nodes are set up and administered using the Central Management functions of Web Gateway.

  - **System files** — These files contain particular parameters of the appliance system. They can be modified using the File Editor.

  - **Update schedules** — Updates are scheduled to ensure that the latest available information is used by the filtering functions on Web Gateway.

System configuration can also include several other activities, such as bonding network interfaces or setting up IP addresses for static routes.

**Contents**

- Initial system settings
- System settings
Initial system settings

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.

The following table shows the settings that are configured at the initial setup and their default values. You can leave these settings at their default values or configure your own settings.

Table 3-1  Initial system settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary network interface</td>
<td>eth0</td>
</tr>
<tr>
<td>Autoconfiguration with DHCP</td>
<td>yes</td>
</tr>
<tr>
<td>Host name</td>
<td>mwgappl</td>
</tr>
<tr>
<td>Root password</td>
<td>&lt;none&gt;</td>
</tr>
<tr>
<td>Remote root logon with SSH</td>
<td>on</td>
</tr>
<tr>
<td>Default gateway</td>
<td>&lt;configured by DHCP&gt;</td>
</tr>
<tr>
<td>DNS server</td>
<td>&lt;configured by DHCP&gt;</td>
</tr>
</tbody>
</table>

For more information about the initial setup of an appliance, see the Setting up Web Gateway chapter of the McAfee Web Gateway Installation Guide.

System settings

System settings are configured on the Appliances tab. You can select them from the navigation pane on this tab. They are listed and described here in alphabetical order.

The following system settings are not listed and described here, but in the chapters that deal with the respective field of web security.

- Anti-Malware system settings, see under Web Filtering.
- Bandwidth Control settings, see under Supporting functions.
- Central Management settings, see under Central Management.
- ePolicy Orchestrator settings, see under Monitoring.
- Hardware Security Module settings, see under Web filtering.
- Kerberos Administration settings, see under Authentication.
- Log File Manager settings, see under Monitoring.
- Proxies settings, see under Proxies.
System settings overview

System settings can be configured in different fields.

- **Licensing and cloud usage** — Settings for licensing and cloud usage are configured on an individual appliance. They are then distributed to any other appliance that runs as a node in a Central Management cluster together with this appliance.
  
  Settings: License, Tenant Info, Web Hybrid

- **General services** — General services settings are used to configure functions such as date and time or the user interface on an appliance system.
  
  Settings: Telemetry, Date and Time, File Server, User Interface

- **Network** — Network settings are configured to integrate the appliance system into your network.
  
  Settings: Proxies, Network Interfaces, Domain Name Service, Network Protection, Port Forwarding, Static Routes.

- **Central Management** — Central Management settings allow you to set up and maintain multiple appliances that run as nodes in a cluster.
  
  Settings: Central Management

- **Authentication and quota management** — Settings for authentication and quota management control web access and usage for the users of your network.

  System settings are configured to cover parts of the authentication and quota management process that are not controlled by policy settings, for example, use of the Kerberos authentication method.

  Settings: Kerberos Administration, Windows Domain Membership, Quota

- **Web filtering** — Web filtering settings control web access and usage regarding particular types of web objects for the users of your network.

  System settings are configured to cover parts of the web filtering process that are not controlled by policy settings, for example, the queue of working threads in Anti-Malware filtering.

  Settings: Anti-Malware, Hardware Security Module

- **Monitoring and troubleshooting** — Settings for monitoring and troubleshooting control the log file manager and enable or disable tracing functions.

  The monitoring process is also controlled in parts by policy settings.

  Settings: Log File Manager, ePolicy Orchestrator, SNMP.
Network interface bonding

Bonding two or more network interfaces enables them to act as one while increasing bandwidth and providing High Availability.

The network interfaces on Web Gateway, for example, the eth2 and eth3 interfaces, can be bound together to form a single channel. A bonding kernel module is created this way and made accessible through a common network interface, which is referred to as the bonding interface.

The network interfaces that are bound together under the bonding interface are referred to as the bonded interfaces. These interfaces can be provided by different NICs.

The terms "master" and "subordinate" are also used to refer to a bonding and a bonded interface, respectively. In some system messages, you will also see the term "slave" used for a bonded interface.

With regard to the components and processes that are involved, network interface bonding is also known as NIC bonding, ethernet bonding, or channel bonding.

You can configure network interface bonding on the user interface of Web Gateway. To verify that a bonding interface has successfully been configured, you can run some suitable commands from a system console.

A VLAN can be configured on a bonding interface in the same way as on an ordinary network interface, using the relevant configuration options of the user interface.

Configure network interface bonding

To configure network interface bonding, create a bonding interface and configure parameters for this interface and the bonding configuration.

Task

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to configure network interface bonding on and click Network Interfaces.

   The Network Interfaces settings appear in the configuration pane.
3. Create a bonding interface.
   a. Under Enable these network interfaces, select a network interface that you want to run as a bonded interface, for example, eth2.
   b. On the Advanced tab, select Bond enabled and in the Name field type the name of the bonding interface that you want to create, for example, bond1.

      Repeat substeps a and b for another network interface that you want run as a bonded interface under this bonding interface.

      You can also add further network interfaces as bonded interfaces and have more than two network interfaces in the bonding configuration.
   c. Click Save Changes.
   d. Log out and log on again.

      After the logon, the new bonding interface appears in the list under Enable these network interfaces.
4 Configure parameters for the bonding interface.
   a Select the bonding interface and click the IPv4 or IPv6 tab, according to the protocol version that is used in your network.
   b Select Configure manually and under IP address and subnet mask type an IP address and the values for a subnet mask.
      You can leave the default value under MTU, which specifies the maximum number of bytes in a single transmission unit, as it is.

5 Configure parameters for the bonding configuration.
   a Select the bonding interface and click the Advanced tab.
   b Under Mode, select one of the following bonding modes.
      • Active/Passive — In this mode, only one bonded interface in the bonding configuration is active at any time. A different bonded interface becomes active only if the active bonded interface fails.
         The MAC address of the bonding interface is only visible externally on one port, which avoids address confusion for a network switch.

         This mode is referred to in some system messages as mode 1.

         The mode is selected by default.

      • 802.3ad/LACP — In this mode, all bonded interfaces in the bonding configuration are active.
         The bonded interface for outgoing traffic is selected according to the configured hash policy.

         This mode is referred to in some system messages as mode 4.

         When this mode is selected, the LACP rate and Hash policy options become accessible.
   c Under Mimon, configure monitoring for the bonding interface.
      The value that you configure here sets the time interval (in milliseconds) for sending the polling messages of the MII monitoring program.
      The default interval is 100 milliseconds.
   d If you have selected 802.3ad/LACP as bonding mode, select options that are specific to this mode.
      Under LACP rate, select the transmission rate for the LACP-DU data packets that are exchanged between bonding and bonded network interfaces.
         • Slow — With this transmission rate, data packets are sent every 30 seconds.
            This transmission rate is selected by default.
         • Fast — With this transmission rate, data packets are sent every second.
      Under Hash policy, select one of the following options.
         • Layer2 — This policy uses a combination of layer 2 values to calculate the hash. The values that are included in this combination are hardware MAC addresses and packet type ID addresses.
            This hash policy is selected by default.
         • Layer2+3 — This policy uses a combination of layer 2 and layer 3 protocol information to calculate the hash.

6 Click Save Changes.
Checking the bonding configuration

You can verify that you have successfully configured a bonding network interface from a system console. To verify that the bonding configuration runs with the parameters that you have configured, you can use a suitable network script. An additional command enables you to check the status of the bonding interface and the network interfaces that are bound to it.

Verifying the configuration parameters

The `ifcfg` network script allows you to verify that the network interfaces of the bonding configuration are running with the configured parameters, such as the bonding mode or the IP address of the bonding interface.

To view the parameters for the bonding interface, for example, `bond 1`, run the network script using the following command:

```
cat /etc/sysconfig/network-scripts/ifcfg-bond1
```

The command returns, for example, the following lines.

```
### BEGIN AUTOGENERATED CONFIG
BONDING_OPTS:='mode=1 miimon=600'
BOOTPROTO='none'
DEVICE='bond1'
IPADDR='10.11.12.12'
...
```

To view the parameters for a bonded interface, for example, `eth2 1`, run the following command:

```
cat /etc/sysconfig/network-scripts/ifcfg-bond1
```

The command returns, for example, the following lines.

```
### BEGIN AUTOGENERATED CONFIG
BOOTPROTO='none'
MASTER='bond1'
SLAVE='yes'
DEVICE='eth2'
...
```

Checking the network interface status

You can check whether the bonded network interfaces are running properly under the bonding interface and which of the bonded interfaces is currently in active (slave) status.

Run the following command, for example, if the bonding interface is `bond1`:

```
cat /proc/net/bonding/bond1
```

The command returns, for example, the following lines.

```
### Ethernet Channel Bonding Driver: v. 3.7.1 (April 27, 2015)
Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
MII Status: up
MII Polling Interval (ms): 600
Up Delay (ms): 0
Down Delay (ms): 0
Slave Interface: eth2
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW Addr: 00:0c:29:e0:a7:37
Slave Queue ID: 0
```
Source-based routing

When configuring routing for traffic in your network, you can let routing decisions be based on the source IP address. This routing method is known as source-based routing.

Using this method you can separate the management traffic that an administrator creates when accessing the user interface of a Web Gateway appliance from the traffic that the administrator or end users create when accessing the web. The two kinds of traffic can also be protected by a separate firewall for each of them.

To implement the method, you allow administrator access to the user interface only through a particular network interface on the appliance. This network interface is the management network interface, while a different network interface is configured for access to the web.

You can also configure that monitoring information, for example, SNMP messages, must access the appliance through the management network interface.

After passing through the management interface, traffic can be identified for further routing by its source IP address, which is the address of the management interface.

Configuring the routing for this traffic includes two main steps:

• Configuring a routing table
• Configuring a route within this table

The source IP address is specified in both steps to ensure that traffic with this address is routed according to a particular table and route.

Different routing tables can be configured and entered in a list on Web Gateway while different routes can be configured for each table.

You can configure routes for use under IPv4 or IPv6, depending on which version of this protocol is followed within your network.

Configure source-based routing for a management network interface

Configure source-based routing to separate other traffic from traffic that has a management network interface as its source.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure source-based routing on.

3. Configure use of the management network interface for administrator access to the user interface.
   a. Click User Interface.
   b. Under HTTP Connector, proceed as follows.
      • Make sure Enable local user interface over HTTP is selected.
      • In the HTTP connector field, type the IP address and listener port of the management network interface.
4 Configure use of the management network interface for SNMP messages.
   a Click SNMP.
   b Under SNMP Port Settings, click the Add icon on the toolbar of the Listener address list.
      The Add SNMP Listeners window opens.
   c In the Listener address field, type the IP address and listener port of the management network interface.
   d Click OK.
      The window closes and the listener address appears in the list.

5 Configure source-based routing for traffic that is sent and received through the management network interface.
   a Click Static Routes.
   b Under Source-based routing, select Source-based routing for IPv4 or Source-based routing for IPv6, depending on the IP version used in your network.
      Two lists for configuring source-based routing appear.
   c On the toolbar of the Static source routing table number list, click the Add icon.
      The Add ApplianceSourceBasedRoutingTable window opens.
   d Configure an entry for the routing table as follows.
      • In the Source information to look up routing table field, type the IP address of the management network interface.
      • In the Routing table number field, type the number of the routing table for the traffic that is sent and received through the management network interface.
   e Click OK.
      The window closes and the routing table entry appears in the list.
   f On the toolbar of the Source-based routing list for IPv4 (or the list for IPv6), click the Add icon.
      The Add ApplianceSourceBasedRoutingIPv4 window (or the window for IPv6) opens.
   g Configure a routing entry as follows.
      • In the Destination field, type the IP address range in CIDR notation for the destinations of the traffic that is sent through the management network interface.
      • In the Routing table number field, type the number of the routing table for the traffic that is sent and received through the management network interface.
      • In the Gateway field, type the IP address of the gateway for the traffic that is sent and received through the management network interface.
• In the **Device** field, type the name of the network interface that you want to configure as the management network interface.

• In the **Source IP** field, type the IP address of the network interface that you want to configure as the management network interface.

6. **Click OK.**

   The window closes and the routing entry appears in the list.

---

**Cache volume resizing**

Logical volumes for web caching and for storing temporary and log files can be resized on an appliance using a wizard.

After Web Gateway has been installed on an appliance, the logical volume for web caching is larger than that for storing temporary and log files. The appliance volume wizard is provided, which allows you to change this sizing and provide more disk space for storing temporary and log files.

Volume size is shown on the wizard pages in GiB. Before the resizing, sizes could be, for example, as follows:

- Web cache volume: 197 GiB
- Temporary and log files volume: 40 GiB

After the resizing the size relation is inverted:

- Web cache volume: 40 GiB
- Temporary and log files volume: 197 GiB

The wizard guides you through the resizing when you set up a Web Gateway appliance for the first time. After completing work with the configuration wizard that is provided for configuring initial system settings, the appliance restarts and the wizard appears.

If the wizard process is interrupted, you can restart it from the command line of a system console using the following command:

```
mwg-cache-wizard
```

When the `yum upgrade` command is used to set up an appliance, the wizard must also be started manually.

The path and file name for the main log that records the activities of the wizard are `/var/log/resize-cache.log`.

If the resizing has already been performed on an appliance, the wizard displays a corresponding message.

If you still need to resize the appliance volumes, contact McAfee support.

---

**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.

To edit system files, only use the File Editor. If you open these files outside the File Editor to edit them manually, your changes will be overwritten when an upgrade to a new version of Web Gateway is performed.

Update handling

Information retrieved from databases and lists 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 from particular sources, such as databases and lists. Examples for these sources and the information that is retrieved from them include the virus signatures that are used in anti-malware filtering, which are stored in DAT files and located in an external database.

Another example is the list of public domain name suffixes, which is used when URLs are analyzed to find a domain suffix based on the host name that is contained within a URL.

There are different methods of updating this information.

• **Manual engine update** — You can manually update 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 external databases. 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.
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.
3. Scroll down to Automatic Engine Updates and configure update settings as needed.
4. Click Save Changes.

**Closed network updates**
Web Gateway appliances can be operated and updated in networks that have no internet connectivity for security or other reasons. These networks are also known as "closed" or "isolated" networks.
When appliances that run in these networks need to be updated, they cannot connect to the usual McAfee update servers. An offline update procedure must be performed instead.
You can select and download an update package from a McAfee portal that is provided for this purpose, store it on portable media and use this media to apply the update package to one or more appliances in a closed network.
Update packages contain updated information for modules (engines) and malware patterns used in the filtering process on an appliance. Only full updates (as opposed to incremental updates) are made available on the portal.
After entering the portal, you need to submit the version number of Web Gateway on the appliance you want to update, and are provided with a list of features that updated information is currently available for.
According to your selection, an update package including all files required for the update is created in zipped format for downloading.
Update an appliance in a closed network

To update an appliance in a network with no internet connectivity, download an update package, store it on portable media, and use the media to perform the update.

Task
1  Download an update package.
   a  Use a browser to go to the update page of the Content & Cloud Security at:
      https://contentsecurity.mcafee.com/update
   b  On the update page, enter the version number for an appliance you want to update.
      A list of features that updated information is available for appears.
   c  Select the features you want to update.
      An update package is created according to your selection.
   d  Download the update package to your system.
2  Use portable media, for example, a USB drive, to transfer the update package from the system you used for the download to your administration system in the closed network.
3  For each appliance in the closed network that you want to update, perform the following steps:
   a  Select Configuration | Appliances.
   b  Click Update Engines, then select Upload Update File.
      The Engine Update by File Upload window opens.
   c  Click Browse, go to the location on the administration system where you stored the update package, and select the update package file.
   d  Click Update.
      The appliance is updated using the information from the update package.
   e  Click Close to close the window.
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
- Explicit proxy mode
- Best practices - Configuring the Proxy HA mode
- Best practices - High Availability configuration size limits
- Best practices - Configuring the explicit proxy mode with WCCP
- Transparent router mode
- Transparent bridge mode
- Packet size handling
- Configure servers for ICAP communication
- Secure ICAP
- SOCKS proxy
- Instant messaging
- XMPP proxy
- Configure common proxy settings
- Controlling outbound source IP addresses
- Best practices - Configuring FTP over HTTP
- Using WCCP to redirect FTP traffic
- Using the Raptor syntax for FTP logon
- Node communication protocols
- Using DNS servers according to domains
- Using DXL messages to exchange web security information
- Best practices - Working with the user-agent header
- Bypassing for Office 365 and other Microsoft services
- Reverse HTTPS proxy
- Proxy auto-configuration
- Using the Helix proxy
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
   • Configure a different network protocol.
     You can add one or more of the following to HTTP (or add them and disable HTTP):
     • HTTPS
     • FTP
     • IFP
     • 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.

![Diagram of explicit proxy mode](image)

**Figure 4-1  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
     - 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**.

**Best practices - Configuring the Proxy HA mode**

The Proxy HA network mode that can be configured on Web Gateway is an explicit proxy mode with High Availability functions. It allows you to perform failover and load balancing without using external load balancers.

**Director node and scanning nodes**

One of the appliances in a Proxy HA configuration is configured as the director node. The other appliances are then configured as scanning nodes. The role is assigned to each appliance by configuring a priority value.
The director node performs load balancing within the High Availability cluster by distributing load to the scanning nodes. Usually, the director node also acts as a scanning node. The scanning nodes can act as backup nodes to replace a failed director node. You can also configure a node as a simple scanning node that does not perform backup functions.

The node that has the director role at a given point in time is known as the active director. The active director uses a virtual IP address (VIP) as an alias IP address on its interface for communication with the clients.

We recommend that you also configure the appliances you want to include in the Proxy HA configuration as members of a Central Management configuration.

These configurations do not depend on each other for running successfully. But if the appliances are not controlled and synchronized by Central Management, each appliance might follow different web security rules after some time.

**Load balancing**

Load balancing in a Proxy HA configuration takes into account resource usage and active number of connections. So, if one scanning node is overloaded, others get more traffic to compensate.

When load balancing is performed, requests from the same client usually go to the same scanning node.

**Failover**

If the director node fails, the backup node with the highest priority takes over the director role. When the original director node returns to active status, it takes over the director role again.

To verify that nodes are available, VRRP (Virtual Router Redundancy Protocol) is used for health checks. You must configure the following for VRRP on each appliance to enable the health checks: A VRRP interface and a virtual router ID that is the same for all members of the High Availability cluster.

Each node sends a multicast packet per second to IP address 224.0.0.18. If no multicast packet from the active director is seen for 3–4 seconds, a failover is performed. The failover lets the backup node with the highest priority become the director node. This node takes on ownership of the virtual IP address of the High Availability cluster and informs the other nodes about its new director role.

Gratuitous ARP (Address Resolution Protocol) messages are used to update the ARP tables of participating clients and routers. Each time the common virtual IP address changes ownership (a failover occurs), the new director node sends a gratuitous ARP message. Subsequent TCP/IP packets can then reach this node.

**Configure the Proxy HA mode**

Configure the Proxy HA mode to perform load balancing and failover without using external load balancers.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select an appliance that you want to include in the Proxy HA configuration, then click **Proxies (HTTP, HTTP(S), FTP, SOCKS, ICAP ...)**.
3. Under **Network Setup**, select **Proxy HA**.
   
   The **Proxy HA** settings appear immediately below the **Network Setup** settings.
4 Configure Web Gateway the following for each appliance in the Proxy HA configuration:

a **Port redirects** — Add an entry with the following parameters in the list of port redirects.
   - **Protocol name** — HTTP
   - **Original destination ports** — Proxy port that the users of your network select in their browsers
   - **Destination proxy port** — Proxy port used by Web Gateway

   The proxy port that the users select in their browsers and the proxy port that Web Gateway uses can be the same, for example, 9090.

   In this case, enter a port redirect into the list that redirects, for example, port 9090 to port 9090.

b **Director priority** — Set a numerical value for the priority in taking the director role.
   - Highest priority, for example, 99 — For the director node
   - Lower priority, must be higher than 0, for example, 89 — For a backup node

   A backup node can perform a failover to replace the director node when that node fails and no other node with a higher priority is available. Otherwise the backup node works as a scanning node.
   - 0 — For a node that only acts as a scanning node

c **Management IP** — Specify the local IP address of the appliance.

   This IP address is used to auto-discover the scanning nodes. All nodes must be on the same subnet to be auto-discovered.

d **Virtual IPs** — Specify the shared IP address for the High Availability cluster.

   This address is owned by the active director and must be the same on all nodes. Your users must select this address in their browsers.

e Configure the settings for the VRRP health checks.
   - **Virtual router ID** — ID used for the VRRP health checks

     This ID must be the same on all nodes. It is 51 by default.

     You can leave the default ID, unless you are already using VRRP elsewhere in your network with ID 51. Then change it here to make it unique for the Proxy HA configuration.

   - **VRRP interface** — Interface used by VRRP for the health checks

     This interface is eth0 by default.

     You can leave the default interface, unless you are not using the eth0 interface on your appliances at all or want to use multiple interfaces.

5 Click **Save Changes**.

When the size of data packets is handled in a flexible manner between a Web Gateway appliance and its clients, using the method known as **Path MTU discovery**, an additional configuration effort is required for the Proxy HA mode.
Resolving issues with a Proxy HA configuration

Several measures can be taken when trying to resolve issues with a Proxy HA configuration.

Look up VRRP health check messages

Messages about the VRRP health checks are logged on an appliance system under:

/var/log/messages

These messages also inform you about whether an appliance is in director or backup node status.

Find out which node blocked a request

To find out which of the nodes in a High Availability cluster blocked a request, edit the user message template for Block actions. Insert the System.HostName property.

Test a specific node

To test the behavior of a particular node, enter a new proxy port in the port redirect list only on that node, for example, 9091.

Then point the browser on the client system that you are using to test the node to <IP address of Web Gateway>: 9091.

Identify the active director

To identify the active director node that owns the virtual IP address of the High Availability cluster, set up an SSH session with each node. Then run the ip addr show command on each of them.

Inspect failure to distribute web traffic

If all web traffic is processed on the director node or another single node instead of being distributed to other nodes, it could have these reasons:

• No port redirects are configured on the director node. If there are no port redirects, the director node will not redirect traffic to other nodes, but handle it locally.

• The director node does not know about any other nodes because they are configured with IP addresses that do not belong to the same subnet.

• All traffic is coming from the same source IP address because there is a downstream proxy or a NAT device in place. Then the usual behavior for load balancing is to direct this traffic to the same node again and again.

Best practices - High Availability configuration size limits

When configuring the Proxy HA (High Availability) network mode, you need to consider the number of Web Gateway appliances to include in the configuration.

In most cases, multiple appliances are run in a network and configured as nodes that are administered using Central Management functions.

Usually, one of these nodes is configured as the director node that directs incoming web traffic to the other nodes, which are termed scanning nodes since their job is to scan this traffic.

On a particular appliance, network interfaces are usually configured in a two-leg solution, which uses separate interfaces for incoming and outgoing web traffic, or in a three-leg solution, which uses an additional interface for Central Management communication.
Considering a network that is configured in this way, the following should be taken into account:

- The number of scanning nodes must be chosen in a way that lets their added maximum throughput not exhaust or exceed the maximum throughput that can be achieved by the director node, which is 1 gigabit per second by default.

  This value results from the following internal restrictions: The network interface that the director node uses by default is limited to processing a data volume of 1 gigabit per second.

  Also, the kernel-mode driver of the MLOS operating system, which runs on a Web Gateway appliance, only allows a scaling of up to 1 gigabit per second.

- We recommend that you leave a clear safety margin when configuring the number of scanning nodes that would theoretically be possible under these conditions.
  - For example, with a throughput of 100 megabits per second for a scanning node, ten nodes would be possible, but we recommend five.
  - With a throughput of 300 megabits per second, three nodes would be possible, but we recommend two.

  The maximum throughput on a scanning node varies with the appliance model that is used as a node and how a node is configured, for example, whether anti-malware filtering or the web cache are enabled or not. To find this value for a node, you can use a sizing calculator.

  Calculations look different if a 10G network interface is used by a director node instead of the default 1G network interface or if IP spoofing is enabled in a configuration. This is explained in the following.

### 10G network interfaces

When a 10G network interface is installed on an appliance that is configured as the director node, the maximum throughput for this node is increased. However, the scaling limit of the MLOS kernel-mode driver must still not be exhausted or exceeded.

- For example, with a throughput of 100 megabits per second for a scanning node, more than five nodes are possible, but we still recommend not to extend their number to ten.
- With a throughput of 300 megabits per second, three nodes are possible, we recommend not to use more.

### IP spoofing

When IP spoofing is configured, data packets pass through the director node twice, once when the director node directs them to the scanning nodes and a second time when they are returned from the scanning nodes to the director node, as this node forwards the data packets to their original IP addresses.

This means the maximum throughput is only 500 megabits per second on the director node if a 1G network interface is used while the scaling limit of the MLOS kernel-mode driver remains the same.

The number of scanning nodes must be adapted accordingly.

- For example, with a throughput of 100 megabits per second for a scanning node and a director node that uses a 1G network interface, the number of scanning nodes must be less than five.
  
  If a 10G network interface is used, the number of scanning nodes can be higher, but we still recommend five.
  
- With a throughput of 300 MBit/s for a scanning node and a director node that uses a 1G network interface, there should be only one scanning node.
  
  If a 10G network interface is used, we recommend not to configure more than three scanning nodes.
Best practices - Configuring the explicit proxy mode with WCCP

When implementing the explicit proxy mode on a Web Gateway appliance, you can configure the redirection of web traffic to Web Gateway under WCCP (Web Cache Communication Protocol). Use of this protocol considerably enhances the capabilities for load balancing and failover.

To enable redirection under WCCP, a suitable router must be placed between the client systems of the users in your network and the web. The router redirects requests for web access from the clients that are directed to particular ports to the Web Gateway appliance.

The router is also referred to as the WCCP device. Instead of a router, you can also use a switch as WCCP device.

On the appliance, you must configure a WCCP service. When configuring this service, you specify a service ID, the IP address of the router, the ports that requests are redirected from, and other information.

Multiple appliances can connect to the same router under WCCP for load balancing and failover. The appliances must be configured as nodes in a Central Management configuration and a WCCP service must be configured on each of them.

The redirection happens transparently, which means users are not aware that their requests are redirected. When the response to a request is received from a web server, Web Gateway forwards it to the client, using (spoofing) the IP address of the web server.

To start working with the router, Web Gateway subscribes to it. The router is not aware of Web Gateway until the subscription happens. No settings must be configured on the router to inform it about Web Gateway.

Communication between Web Gateway and the router

Under WCCP, data packets are exchanged to subscribe, negotiate settings, and as health checks. Web Gateway sends a "Here I Am" packet to the router and forwards the configured settings. These settings include the ports for redirection, the ID of the WCCP service, the IP address that traffic should be redirected to, and other information.

The router acknowledges with an "I See You" packet that the subscription has been successful and includes the router ID, which is the highest interface IP address on the router.

If a router does not receive a "Here I Am" packet over more than 25 seconds, it sends a removal query, requesting that Web Gateway respond immediately. If no response is received within another 5 seconds, Web Gateway is considered offline and removed from the pool of WCCP partners.

Load balancing and failover

In a WCCP configuration with multiple Web Gateway appliances, the first appliance that connects to the router distributes workload to the other appliance. Portions of workload that are distributed are also known as "buckets" in WCCP terminology.

When an appliances goes offline or returns, buckets are immediately reassigned. If the appliance that is currently assigning buckets goes offline, another appliance takes over its role.

We do not recommend using WCCP when the router, client systems, or the Web Gateway appliances are separated by a device that uses the method known as source NATing to handle client traffic. This method impacts the performance of load balancing under WCCP. It also prevents you from configuring rules for user authentication based on time or client IP addresses.

Fail-open and fail-closed strategies

If use of the WCCP protocol is configured on the router and no Web Gateway appliance is available, the router lets requests for web access pass through without redirection. This behavior follows a strategy known as fail-open strategy.
If you have a firewall in your network, you must configure it to allow requests for web access with any source IP addresses to enable this strategy. Requests can then go out to the web directly.

Under a fail-close strategy, requests are blocked if no Web Gateway appliance is available to redirect them to. For this strategy to work, you must configure the firewall to allow only requests with source IP addresses belonging to Web Gateway.

**Using WCCP only or as fallback solution**

You can use the explicit proxy mode with WCCP as your only network mode solution, which means all web traffic is handled in this mode. You can also use it as a fallback solution for special use cases in an explicit proxy configuration, for example, to deal with applications that do not recognize proxy settings. Another use case would be handling web traffic in a Wi-Fi network segment where users can bring their own devices.

As best practice, we recommend using two different proxy ports. Configure one for handling web traffic in explicit proxy mode with WCCP, and one for handling it without WCCP. Following this practice allows you to use the property for proxy ports in the criteria of web security rules.

**Configure use of the WCCP protocol**

To configure use of the WCCP protocol, configure a router and one or more Web Gateway appliances for handling web traffic according to this protocol.

**Task**

1. Configure a router for handling web traffic according to the WCCP protocol.
   Configuring the router mainly includes specifying the ID of the WCCP service. For more information, see the router documentation.

2. Configure a Web Gateway appliance for handling web traffic according to the WCCP protocol.
   Configuring the appliance mainly includes setting up a WCCP service on it.
   a. Select Configuration | Appliances.
   b. Select the appliance that you want to configure for use of the WCCP protocol and click Proxies (HTTPS, FTP, SOCKS, ICAP ...).
   c. Under Network Setup make sure that Proxy (optional WCCP) is selected. Under Transparent Proxy select WCCP. The WCCP services list appears.
   d. On the list toolbar, click the Add icon.
      The Add WCCP Service window opens.
   e. To add a service, provide values for the service parameters. When you are done, click OK.
      The new service appears in the WCCP services list.
   f. Click Save Changes.
You can include more than one appliance in a WCCP configuration. Configure a WCCP service on every appliance that you want to include.

When configuring the explicit proxy mode with WCCP after using a different network mode before (Proxy HA mode, transparent router or bridge mode), you must restart the appliance.

The restart unloads the network driver that handles the transparent interception and redirection of web traffic. Restarting is only required once. Later on you can enable and disable use of the WCCP protocol without restarting.

**Settings for a WCCP service**

When configuring the settings for a WCCP service, you specify values for several service parameters. Regarding these parameters, consider the best-practice information that is provided in the following.

**Service ID**

The service ID identifies the WCCP service. The service is also included in the configuration of the router, where the ID for this service must be the same.

Service IDs 0–50 are static under WCCP and reserved for well known services with standard configurations. Service IDs 51–255 are dynamic and involve negotiation between the partners in the WCCP configuration. For the WCCP service that you configure, we recommend using a value from 51 to 98.

**WCCP router definition**

The IP address of the router that is used in the WCCP configuration is specified in the router definition. Alternatively, you can specify the name that this IP address is resolved to by a domain name server.

You can configure multiple routers by specifying an IP address or DNS name for each of them or by using a multicast IP address. The use of an IP address as multicast IP address for multiple routers is indicated in the configuration of the respective routers by specifying the keywords `group-address` and `group-listen`.

**Ports to be redirected**

The ports that web traffic is redirected from to the Web Gateway proxy port are listed here.

The redirection works for traffic under the HTTP protocol and also under HTTPS. Redirection of FTP traffic or traffic under any other protocol is not supported. This means that all ports that you list here must be ports for HTTP and HTTPS traffic. Port 80 for HTTP traffic and port 443 for HTTPS traffic are by default included in the list.

If you add more ports for HTTPS traffic, you must also add them as ports that are to be treated as SSL within the HTTP proxy configuration.

If version 1 of WCCP is used, only traffic for port 80 is redirected. You cannot add any other ports for redirection.

**Proxy listener address**

The proxy listener address is the physical IP address of the network interface card on a Web Gateway appliance that web traffic is redirected to.

**Proxy listener port**

The proxy listener port is the port on Web Gateway that listens to the redirected requests.

For the redirection to work, you must bind the proxy listener port to the IP address 0.0.0.0. For example, if you are using the default port 9090, bind it by specifying 0.0.0.0:9090.
You must not bind the port (by specifying localhost) to the IP address of the appliance that you are working on, nor to any other IP address. Otherwise the redirection will not work and traffic will not be processed.

**Assignment method**
The assignment method is the method for assigning buckets (processing jobs) under WCCP to different Web Gateway appliances when a configuration consists of more than one appliance. The method can be assignment by mask or hash. Some routers only support the mask assignment method. For more information, see the router documentation.

**Input for load distribution**
Load distribution can based on the source or destination IP address or the source or destination port of a request. We recommend configuring load distribution based on the source IP address. This ensures that the same appliance is always used for the requests that a user submits from a particular client system. Breaking sessions is avoided this way.

**Assignment weight**
The assignment weight is used to assign traffic load to different Web Gateway appliances in a WCCP configuration. If the default value 1000 is configured on all appliances, the load is distributed equally.

If an appliance in the configuration performs better than the others, you can configure a higher value on this appliance and lower values on the others. If all appliances perform equally well, we recommend leaving the default value on each of them.

**GRE-encapsulated**
When the Generic Routing Encapsulation (GRE) method is used for sending data packets, an original data packet is encapsulated inside a new packet with additional headers. The new packet is then sent from the router to Web Gateway over a connection that is known as a GRE tunnel. This method requires more overhead, but has the advantage of working across subnets.

**L2-rewrite to local NIC**
When the L2-rewrite (Layer 2 rewrite) method is used for sending data packets, the destination MAC address is rewritten to the MAC address of the proxy. The packets are then redirected to a network interface on an appliance. This method works only if the router and the appliance are on the same subnet.

**L2-redirect target**
The target for redirecting data packets under the L2-rewrite method is the network interface of a NIC on the appliance that you are working on. The interface name, for example, etho, is selected to specify this interface.

**Troubleshooting WCCP-related issues**
You can review WCCP-related information on the appliance dashboard or retrieve it running suitable commands on the command line of a system console that is connected to the appliance.

**Review WCCP-related information on the dashboard**
Review WCCP-related information on the dashboard, to see whether troubleshooting activities are required.

**Task**
1. Select Dashboard | Charts and Tables.
2. On the navigation pane, click System Summary and scroll down to the WCCP Service Current Status Report table.
The table shows values for several WCCP parameters, such as the ID of the WCCP service that the appliance has subscribed to, the IP address of the router, forwarding and return methods, and assigned buckets.

It also shows the time stamps of the latest "Here I Am" and "I See You" data packets, which allows you to verify that the health check is working.

**Retrieving WCCP-related information on the command line**

You can use several commands to retrieve WCCP-related information on the command line.

Enter the following command to see if web traffic is redirected to the configured port on a Web Gateway appliance.

```
iptables -t mangle -L
```

You will see, for example, an entry for the chain **WCCP0** with a line containing `redirect 10.10.73.72:9090`.

10.10.73.72 is the IP address of the network interface of the NIC on the Web Gateway appliance that you configured as destination of the redirected traffic. 9090 is the configured port.

You can check whether the appliance sends "Here I Am" and "I See You" data packets. Enter the following command:

```
tcpdump -npi eth0 port 2048
```

Within the data packets that are displayed, verify that the following applies:

- The IP address shown for the web cache is the IP address of the Web Gateway appliance.
- The bucket assignment method is the method that is also configured for Web Gateway.
- The redirect method is the method that is also configured for Web Gateway.

You can check whether the GRE-encapsulated or L2-rewritten data packets are received on the Web Gateway appliance.

- For GRE-encapsulation, enter the following command:
  ```
tcpdump -npi eth0 ip proto 47
  ```
  Verify that the source IP address of the data packets is the IP address that is configured for the router on Web Gateway.

- For L2-rewriting, enter the following command:
  ```
tcpdump -npi eth0 not host <IP address of the Web Gateway appliance
  ```
  Verify that the source IP address of the data packets is the IP address of the client that sent the request.

To check that redirected data packets are received on Web Gateway, you can also enter the `ifconfig` command.

**Transparent router mode**

The transparent router mode is one of the two transparent modes you can configure for the proxy functions of a Web Gateway appliance if you do not want to use an explicit mode.

In transparent router mode, the clients are unaware 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. A switch can be used for connecting the appliance to its clients. A routing table is used to direct the traffic.
Director and scanning nodes

If you are running several appliances as nodes within a complex configuration, for example, in a Central Management cluster, one node is usually configured as director, while the other nodes are configured as scanning nodes.

The director node receives web traffic from the clients and distributes it to the scanning nodes, which perform filtering activities on the traffic according to the rules that are implemented. Further handling of the traffic by the director or scanning nodes differs depending on what is configured. The director node can also perform filtering activities.

If you are only running one Web Gateway appliance in your network and want to configure it in transparent router mode, you must still configure the director role for it to let it receive, filter, and forward web traffic.

Best practice: Configure at least two director nodes to avoid problems in case one of them goes offline.

Configure the transparent router mode

To configure the proxy functions of an appliance in transparent router mode, complete the following high-level steps.

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).
   After selecting this mode, specific Transparent Router settings appear below the Network Setup settings.
   Common settings follow the specific settings, including settings for configuring the HTTP, FTP, and other network protocols.
4. Configure specific and common settings as needed.
5. Click Save Changes.

When running several appliances as nodes in a Central Management configuration, you can configure the transparent router mode on each of them.

Configure nodes in transparent router mode

You can configure the transparent router mode for two or more appliances that are nodes in a Central Management configuration. One of the nodes takes the director role, which means it directs data packets, while the scanning nodes filter them.
Node configuration includes configuring network and proxy settings.
Tasks

- **Configure network settings for a director node in transparent router mode on page 44**
  To configure a director node in transparent router mode, configure network interfaces for inbound and outbound web traffic.

- **Configure proxy settings for a director node in transparent router mode on page 44**
  To configure proxy settings for a director node in transparent router mode, configure the director role for this node, as well as port redirects and proxy ports.

- **Configure a scanning node in transparent router mode on page 45**
  To configure a scanning node in transparent router mode, configure one network interface for outbound traffic. Configure the proxy settings in the same way as for a director node in this mode, except for the scanning role.

**Configure network settings for a director node in transparent router mode**

To configure a director node in transparent router mode, configure network interfaces for inbound and outbound web traffic.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure as a director node and click **Network interfaces**.

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.

**Configure proxy settings for a director node in transparent router mode**

To configure proxy settings for a director node in transparent router mode, configure the director role for this node, as well as port redirects and proxy ports.

The director role is configured by giving the node a priority value > 0.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure as a director node and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3. Under **Network Setup**, select **Transparent Router**.
   Specific **Transparent Router** settings appear below the **Network Setup** settings.

4. Configure one or more port redirects that let requests sent from clients of Web Gateway be redirected to a particular port.
   a. Under **Port redirects**, click **Add**.
      The **Add Port Redirects** window opens.
Configure the following for a new port redirect that applies to connections under HTTP or HTTPS:

- **Protocol name** — http
  
  *http* covers connections under both HTTP and HTTPS.

- **Original destination ports** — 80, 443
  
  These are the default destination ports. They cover connections under both HTTP and HTTPS.

  If you also want to filter HTTPS traffic, enable the SSL Scanner rule set, which is by default provided on the rule sets tree, but not enabled.

- **Destination proxy port** — 9090
  
  9090 is the default proxy port on an appliance.

  If you need to use other ports due to the requirements of your network, change these settings as needed.

  To configure a port direct for connections under FTP, select this protocol. Default ports are then preconfigured, which you can change as needed.

5. Set **Director priority** to a value > 0.

6. In the **Management IP** field, type an IP address for each of the scanning nodes that the director should be able to connect to.

7. Under **Virtual IPs**, configure virtual IP addresses for the inbound and outbound network interfaces, using free IP addresses for this purpose.

8. Leave the number under **Virtual router ID** as it is.

9. From the **VRRP interface** list, select the interfaces for heartbeats under this protocol.

10. Configure IP spoofing as needed.

11. Under **HTTP proxy port**, make sure **Enable HTTP proxy** is selected.

   The setting is selected by default. An entry for port 9090 is also configured by default on the **HTTP Port Definition List**.

   - You can change this port as needed. Clicking **Add** opens the **Add HTTP Proxy Port** window, which allows you to add more proxy ports.

   - To configure one or more FTP proxies, select **Enable FTP Proxy** under **FTP Proxy**. An entry for FTP control port 2121 and FTP data port 2020 is then preconfigured on the **FTP Port Definition List**

12. Click **Save Changes**.

**Configure a scanning node in transparent router mode**

To configure a scanning node in transparent router mode, configure at least one network interface for outbound traffic. Configure the proxy settings in the same way as for a director node in this mode, except for the scanning role.

The scanning role is configured by giving the node 0 as the priority value.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure as a scanning node and click **Network Interfaces**.
3. Configure network interfaces as is suitable for your network. You need at least one interface for outbound web traffic.

4. Click Save Changes.

5. You are logged off and logged on to the appliance again.

6. On the appliances tree, select the appliance you want to configure as a scanning node and click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).


8. Configure the same port redirects as for the director node.

9. Set Director priority to 0.

10. Configure IP spoofing in the same way as for the director node.

11. Configure the same HTTP and FTP proxy ports as for the director node.

12. Click Save Changes.

To run more than one scanning node in transparent router mode, configure additional appliances in the same way.

**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 4-2 Transparent bridge mode](image-url)
Configure the transparent bridge mode
To configure the proxy functions of an appliance in transparent bridge mode, complete the following high-level steps.

**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.
   Common settings follow the specific settings, including settings for configuring the HTTP, FTP, and other network protocols.

4. Configure specific and common settings as needed.

5. Restart the appliance.
   The restart includes the reloading of network drivers, which ensures that the appropriate drivers for this network mode are applied.

   **Best practice:** Restart the appliance also after switching from the transparent bridge mode to another network mode.

6. Click **Save Changes**.

When running several appliances as nodes in a Central Management configuration, you can configure the transparent bridge mode on each of them.

   When the size of data packets is handled in a flexible manner between a Web Gateway appliance and its clients, using the method known as **Path MTU discovery**, an additional configuration effort is required for the transparent bridge mode.

**Configure nodes in transparent bridge mode**
You can configure the transparent bridge mode for two or more appliances that are nodes in a Central Management configuration. One of the nodes takes the director role, which means it directs data packets, while the scanning nodes filter them.

Node configuration includes configuring network, Central Management, and proxy settings.

**Tasks**

- **Configure network and Central Management settings for a director node in transparent bridge mode on page 48**
  To configure a director node in transparent bridge mode, configure a network interface for the transparent bridge functions and let its IP address be used for Central Management communication.

- **Configure proxy settings for a director node in transparent bridge mode on page 49**
  To configure proxy settings for a director node in transparent bridge mode, configure the director role for it, as well as port redirects and proxy ports.

- **Configure a scanning node in transparent bridge mode on page 50**
  To configure a scanning node in transparent bridge mode, configure the same settings as for a director node in this mode, except for the scanning role.
Configure network and Central Management settings for a director node in transparent bridge mode

To configure a director node in transparent bridge mode, configure a network interface for the transparent bridge functions and let its IP address be used for Central Management communication.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure as a director node and click Network interfaces.

3. Prepare the network interface for the transparent bridge functions.
   a. Select a still unused network interface of the appliance, but do not enable it yet.
   b. On the Advanced tab, select Bridge enabled.
   c. In the Name field, type ibr0 as the name of the interface.
   e. Click Save Changes.

You are logged off and logged on to the appliance again.

4. Configure the network interface for the transparent bridge functions.
   a. Select Configuration | Appliances. Then select the appliance again, and click Network interfaces.

An additional network interface named ibr0 is now available.

   b. Select the ibr0 interface.
   c. On the IPv4 tab, configure an IP address, a subnet mask, and a default route for this interface.
   d. Select the checkbox next to the interface to enable it.

5. Configure the network interface that is currently used to access the appliance as the network interface for the transparent bridge functions.
   a. Select the network interface that is currently used to access the appliance.
   b. On the Advanced tab, select Bridge enabled.
   c. In the Name field, type ibr0 as the name of the interface.

6. Enable the ibr0 network interface that you selected in step 3 from the until now unused network interfaces.

7. Configure Central Management settings.
   a. Select Central Management.
   b. Under Central Management Settings, add the IP address you configured for the ibr0 network interface to the list that is provided.

8. Click Save Changes.

If you want to use more than one network interface for the transparent bridge mode, configure more unused network interfaces of an appliance in the same way.
Configure proxy settings for a director node in transparent bridge mode

To configure proxy settings for a director node in transparent bridge mode, configure the director role for it, as well as port redirects and proxy ports.

The director role is configured by giving the node a priority value > 0.

**Task**

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure as a director node and click Proxies (HTTP(S), FTP, ICAP, and IM).

   Specific Transparent Bridge settings appear below the Network Setup settings.

4. Configure one or more port redirects that let requests sent from clients of Web Gateway be redirected to a particular port.
   a. Under Port redirects, click Add.
   b. Configure the following for a new port redirect that applies to connections under HTTP or HTTPS:
      • Protocol name — http
        *http covers connections under both HTTP and HTTPS.*
      • Original destination ports — 80, 443
        *These are the default destination ports. They cover connections under both HTTP and HTTPS.*
        If you want to filter also HTTPS traffic, you need to enable the SSL Scanner rule set, which is by default provided on the rule sets tree, but not enabled.
      • Destination proxy port — 9090
        9090 is the default proxy port on an appliance.
        If you need to use other ports due to the requirements of your network, change these settings as needed.
        To configure a port direct for connections under FTP, select this protocol. Default ports are then preconfigured, which you can change as needed.

5. Set Director priority to a value > 0.

6. In the Management IP field, type the IP address you specified for ibr0 when configuring the network settings.

7. Configure IP spoofing as needed.

8. Under HTTP proxy port, make sure Enable HTTP proxy is selected.
   The setting is selected by default. An entry for port 9090 is also configured by default on the HTTP Port Definition List.
   • You can change this port as needed. Clicking Add opens the Add HTTP Proxy Port window, which allows you to add more proxy ports.
   • To configure one or more FTP proxies, select Enable FTP Proxy under FTP Proxy. An entry for FTP control port 2121 and FTP data port 2020 is then preconfigured on the FTP Port Definition List.

9. Click Save Changes.
Configure a scanning node in transparent bridge mode

To configure a scanning node in transparent bridge mode, configure the same settings as for a director node in this mode, except for the scanning role.

The scanning role is configured by giving the node 0 as the priority value.

**Task**

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure as a scanning node and click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).

   Specific Transparent Bridge settings appear below the Network Setup settings.

4. Configure the same port redirects as for the director node.

5. Set Director priority to 0.

6. Configure IP spoofing in the same way as for the director node.

7. Configure the same HTTP and FTP proxy ports as for the director node.

8. Click Save Changes.

To run more than one scanning node in transparent bridge mode, configure additional appliances in the same way.

**Best practices - Fine-tuning a transparent bridge configuration**

When configuring Web Gateway in transparent bridge mode, you can complete several activities in addition to the basic steps to improve the configuration.

These activities include the following:

- Configuring port redirects
- Setting up more than one appliance
- Appropriate handling of the STP protocol

**Configuring port redirects**

Web Gateway is by default configured to scan and filter requests for web access arriving on ports 80 and 443. All requests arriving on other ports are passed on to the web unfiltered unless you specify additional ports.

You can configure port redirects as exceptions for requests coming from a particular client IP address or going to a particular destination IP address. These exceptions are also passed on to the web unfiltered.

**Setting up more than one appliance**

When configuring Web Gateway in transparent bridge mode, we recommend setting up more than one appliance.

When a Web Gateway appliance is configured in this mode, it is implemented in an in-line position within your network. This means that all traffic is physically passing through the appliance, even if no ports are configured to receive the traffic and enable its filtering. Setting up only one appliance would therefore make it a single point of failure.

If you set up at least one other appliance, it can serve as a failover device. Another appliance will, however, not only perform failover functions, but also load balancing, receiving, and processing web traffic.
Avoiding a port shutdown under STP

When the Web Gateway appliances in your network are directly connected to switches that use the Spanning Tree Protocol (STP), ports needed for load balancing communication might be shut down under this protocol.

On most network switches, STP is used to avoid loops and ensure a single path of communication, shutting down redundant ports that cause such loops.

The protocol is also used, however, when two or more Web Gateway appliances are configured in transparent bridge mode. One of the appliances then takes the director role, in which it directs the web traffic that occurs to the other appliance or appliances for processing.

STP is used to communicate this role and the load balancing measures between the appliances.

If network switches with STP are directly connected to the Web Gateway appliances, it is highly likely that ports needed for this load balancing communication are shut down.

You can proceed in one of the following ways to avoid a shutdown:

- Disable STP on every switch that is directly connected to a Web Gateway appliance.

  Do not use this method if other components of your network rely on these switches and STP.

- Install a second switch without STP between every Web Gateway appliance and every switch with STP that the appliance would be connected to.

  Setting up your network in this way ensures that load balancing on the Web Gateway appliances and other network components that rely on switches with STP are not impacted.

Configure port redirects for the transparent bridge mode

Configure port redirects for the transparent bridge mode to pass on particular requests to the web unfiltered.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure port redirects on and click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).

   The Transparent Bridge settings appear below the Network Setup settings.

4. In the list under Port redirects, specify an IP address and subnet mask for every port redirect that you want to configure.

5. Click Save Changes.

Packet size handling

When communication between Web Gateway on an appliance and its clients requires that the size of data packets is handled in a flexible manner, only the explicit proxy mode can be configured as usual.

The following modes require an additional configuration effort in this case:

- Proxy HA (High Availability) mode
- Transparent router mode
- Transparent bridge mode
The size of data packets is measured by the MTU (Maximum Transmission Unit) parameter, which limits the number of bytes that can be sent in one packet.

The method of negotiating the value for this parameter between communication partners is known as Path MTU Discovery. It is not available for the three modes listed above.

For example, when Web Gateway sends a data packet to a client that it connects to through a VPN (Virtual Private Network) tunnel, the MTU that the VPN tunnel can handle might be 1412, whereas the MTU of the data packets is 1500.

The VPN gateway then sends a message under the ICMP protocol to inform its partner about the required size, but this message cannot be processed unless the configured network mode is the explicit proxy mode.

To solve this problem for the other modes, reduce the MTU parameter value for the network interface on Web Gateway that is used for the communication, in this case, for communication with clients behind a VPN tunnel. Set the parameter to the value that is required, for example, to 1412.

The MTU parameter is configured on the user interface as part of the Network Interfaces settings for the IPv4 or IP6 protocol, which can be accessed under Configuration | Appliances.

---

### Configure servers for ICAP communication

Configure servers for ICAP communication in each of the two ICAP modes by specifying their IP addresses or fully qualified domain names.

When Web Gateway connects as a client to an ICAP server, it selects this server from a list that you must configure. The configuration must be completed for both ICAP modes: REQMOD and RESP. The server is called by a rule in a rule set for handling activities that Web Gateway performs in its role as ICAP client. There is one rule set for the REQMOD and another for the RESP. mode.

**Task**

1. Import the ICAP Server rule set from the library.

2. Select Policy | Rule Sets, then click the ICAP Client rule set.

   The key elements view of this rule set appears in the configuration pane.

3. Configure servers for the REQMOD mode.
   a. Click Edit next to ReqMod server.

      The Edit List (ICAP Server) window opens.

   b. Under List Content, click Add.

      The Add ICAP Server window opens.

   c. In the URI field under ICAP Server, specify a server.

      Type the IP address or the fully qualified domain name of a server, followed by the ICAP mode. Optionally, you can add a port. If you add no port, the default port 1344 is configured.

      The syntax for specifying this information is displayed above the field. For example, you can type one of the following strings:

      - `icap://10.213.246.89/reqmod`
      - `icap://10.213.246.89:1346/reqmod`
You can add more than one server to the list. Web Gateway tries the listed servers one after another until a connection is established.

4. Click OK in each of the two open windows.

5. Click Save Changes.

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 will receive SSL-secured requests from its clients. The clients are not required to submit certificates.

Requests that are 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.

SOCKS proxy

You can configure Web Gateway to run as a proxy that forwards web traffic under the SOCKS (Sockets) protocol. When web traffic goes on under the SOCKS protocol, it also follows an embedded protocol, which can be, for example, HTTP or HTTPS.

The embedded protocol can be detected on Web Gateway, and if filtering is supported for web traffic under this protocol, the configured filtering rules can be processed for this traffic. If filtering is not supported, the traffic can be blocked by a suitable rule.

There are some restrictions to using the SOCKS protocol for the proxy functions on Web Gateway:

- The SOCKS protocol version must be 5, 4, or 4a.
- The BIND method is not supported for setting up connections under the SOCKS protocol.

Web traffic that is forwarded by a next-hop proxy under the SOCKS protocol can be protected using level 1 or 2 of the Kerberos authentication method.

In this case, encryption that would also make this traffic SSL-secured cannot be applied, so SSL scanning is not required. The default SSL Scanner rule set therefore includes a criteria part that lets this traffic skip SSL scanning.
Configuring a SOCKS proxy

To configure Web Gateway as a SOCKS proxy, you need to complete several activities.

• Enable the SOCKS proxy.

• Specify one or more proxy ports that listen to the SOCKS proxy clients when they send requests to Web Gateway.

  These ports are specified as part of the common proxy settings on Web Gateway.

• Create rules that control the behavior of the SOCKS proxy.

  These settings are configured as part of the common proxy settings on Web Gateway.

Using properties and an event in rules for a SOCKS proxy

Two properties and an event are available to create rules for controlling the behavior of Web Gateway when it runs as a SOCKS proxy.

There is no preconfigured SOCKS proxy rule set available in the default rule set system or the rule set library. If you want to use such rules, you need to create them and insert them in an existing rule set or create a rule set for them.

• ProtocolDetector.DetectedProtocol — This property can be used to detect the embedded protocol that is followed in web traffic under the SOCKS protocol, for example, HTTP or HTTPS.

  Its value is the protocol name in string format. When the embedded protocol cannot be detected, the string is empty.

• ProtocolDetector.ProtocolFilterable — This property can be used to find out whether filtering is supported for web traffic following the embedded protocol that has been detected.

  Its value is true if this traffic is filterable and false otherwise.

    If this property is processed in a rule, the ProtocolDetector.DetectedProtocol property is also filled with a value. If this value is an empty string for the latter property, which means no the embedded protocol could not be detected, the value of the ProtocolDetector.ProtocolFilterable property is, consequently, set to false.

• ProtocolDetector.ApplyFiltering — This event can be used to enable processing of other rules that are configured on Web Gateway for filtering web traffic under the protocol that has been detected.

Accordingly, the following rule enables processing of other rules for filtering web traffic under the SOCKS protocol if an embedded protocol has been detected that is filterable.

Name

Enable filtering for SOCKS traffic following an embedded protocol that is filterable

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProtocolDetector.ProtocolFilterable is true</td>
<td>-&gt; StopCycle</td>
<td>ProtocolDetector.ApplyFiltering</td>
</tr>
</tbody>
</table>

The following rule blocks SOCKS traffic if no embedded protocol is detected.

Name

Block SOCKS traffic if no embedded protocol can be detected

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProtocolDetector.DetectedProtocol equals &quot; &quot;</td>
<td>-&gt; Block</td>
</tr>
</tbody>
</table>
If no rule is configured that would enable the filtering of SOCKS traffic or block it if no embedded protocol is detected, this traffic is allowed.

This means that if a request for web access is received from a SOCKS client on Web Gateway, it is forwarded to the requested web server without any further processing.

**Configure SOCKS proxy settings**
You can configure settings for a SOCKS proxy as part of the common proxy settings on Web Gateway.

**Task**
1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to configure as a SOCKS proxy, then click **Proxies (HTTP(S), FTP, ICAP, and IM)**.
   
   The settings for configuring proxy functions appear in the configuration pane.
3. Scroll down to the **SOCKS Proxy** settings.
4. Configure these settings as needed.
5. Click **Save Changes**.

**Using UDP under SOCKS**
You can configure UDP (User Datagram Protocol) when Web Gateway is running as a proxy under the SOCKS protocol.

When traffic going on under the SOCKS protocol is processed by the proxy functions on Web Gateway, traffic that follows UDP can also be detected and forwarded. This traffic is not filtered, but forwarded as it is.

To allow the handling of UDP traffic in this way, you must complete the following configuration activities.

- Set the range of ports that listen to UDP traffic.
- Set a timeout on connections for UDP traffic.

You need not explicitly enable the handling of UDP traffic in addition to configuring these settings, as it is basically enabled by default.

When a client of Web Gateway sends a request for setting up a connection that follows UDP under SOCKS, the command name sent with the request is stored as the value of a property.

The name of the property is **Command.Name** and its value is **SOCKSUDPASSOCIATE** then. You can use this property in a rule for monitoring or other purposes.

> You can also use this property in a rule to disable processing of UDP traffic on Web Gateway.

Use of UDP is also monitored and shown on the dashboard under **SOCKS Traffic Summary**.

**Configure settings for UDP under SOCKS**
Configure settings for UDP to enable filtering of traffic that is going on under this protocol when Web Gateway is running as a proxy under the SOCKS protocol.

**Task**
1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to configure UDP settings on and click **Proxies (HTTP(S), FTP, SOCKS, ICAP ...)**.
In the configuration pane, scroll down to **SOCKS Proxy**. Under **Port range for UDP**, set the range of ports that listen to UDP traffic.

Scroll further down to **Timeouts for HTTP(S), FTP, ICAP, SOCKS, and UDP**. Under **UDP timeout**, set the timeout on connections for UDP.

Click **Save Changes**.

**SOCKS Proxy rule set**

The SOCKS Proxy rule set is a library rule set for filtering traffic that is going on under the SOCKS protocol.

<table>
<thead>
<tr>
<th>Library rule set – SOCKS Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM) and responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

- **Filter traffic under the SOCKS protocol with filterable embedded protocol**
  

  The rule uses the `ProtocolDetector.ProtocolFilterable` property to check whether the protocol that is embedded in the SOCKS traffic is filterable on Web Gateway. Filterable protocols are HTTP and HTTPS.

  If either of these two protocols is detected, filtering is enabled by the rule event. If no embedded protocol is detected, the rule does not apply and processing continues with the second rule.

- **Block traffic under the SOCKS protocol if no embedded protocol is detected**
  
  `ProtocolDetector.ProtocolFilterable <Protocol Detector Settings> equals " "` → Block <Default>

  The rule blocks requests if no embedded protocol is detected.

- **Block traffic under the SOCKS protocol if detected protocol is not on whitelist**
  
  `ProtocolDetector.DetectedProtocol <Protocol Detector Settings> is not in list Protocol Whitelist` → Block <Default>

  The rule blocks requests if an embedded protocol is detected, but is not on a particular whitelist.

  The rule is not enabled by default.

**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)
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`
- `relay1.msg.dcn.yahoo.com`
- `relay2.msg.dcn.yahoo.com`
- `relay3.msg.dcn.yahoo.com`
- `mcs.msg.yahoo.com`
- `scs.msg.yahoo.com`
- `scs.msg.yahoo.com`
- `mcs.msg.yahoo.com`
- `scsa.msg.yahoo.com`
- `scsb.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`
- `scs-foof.msg.yahoo.com`
- `scsd.msg.yahoo.com`
- `scse.msg.yahoo.com`
- `scsf.msg.yahoo.com`
- `scsg.msg.yahoo.com`
- `scsa.msg.yahoo.com`
- `scsh.msg.yahoo.com`
- `scsb.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.

---

**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.

---

**Configure common proxy settings**

You can configure common proxy settings in addition to the specific settings for a network mode. Common proxy settings include settings for the different types of proxies that can be configured on Web Gateway.

**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**.
Controlling outbound source IP addresses

Using different source IP addresses for outbound connections from Web Gateway to web servers or next-hop proxies can lead to connection problems. To avoid these problems, you can replace these addresses with a single address.

Different source IP addresses might be used, for example, when load balancing is configured for multiple Web Gateway appliances. Load balancing can lead to connection problems on the side of the involved web servers or next-hop proxies. Problems can, for example, arise when source IP addresses change during a session period.

To avoid these problems, you can configure a rule that replaces changing source IP addresses with a single address.

This single address does not have to be fixed. You can set up a list of IP addresses and let the rule select an address in a particular position on the list. The address that replaces other addresses then varies according to what you have entered in that position.

Network setups for controlling outbound source IP addresses

Controlling outbound source IP addresses is supported for network setups with:

- IPv4 or IPv6
- HTTP, HTTPS, FTP, or SOCKS proxy
- Proxy (with optional WCCP) mode

The transparent router mode is supported if the source IP addresses that are used for replacing other addresses are configured as aliases.

The Proxy HA and transparent bridge modes are not supported.

Periodic rule engine triggering is also possible when control of outbound source IP addresses is implemented.

Sample rule for controlling outbound source IP addresses

A rule that replaces outbound source IP addresses by a single address, for example, when connections to next-hop proxies are set up, could look as follows:

Name

Use proxy depending on the destination

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL.Destination.IP is in range list Next Hop Proxy IP Range List</td>
<td>Continue</td>
<td>Enable Next Hop Proxy&lt;Internal Proxy&gt;</td>
</tr>
<tr>
<td>OR</td>
<td></td>
<td>Enable Outbound Source IP Override(Proxy.OutboundIP(2))</td>
</tr>
<tr>
<td>URL.Destination.IP is in list Next Hop Proxy IP List</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The criteria of the rule specifies when a next-hop proxy is used. The first of the two events sets up a connection to a next-hop proxy.

The second event, Enable Outbound Source IP Override, is for controlling outbound source IP addresses. It replaces ("overrides") any source IP address that is submitted with a request by an IP address that is taken from a list.
An event parameter, which is itself a property, specifies the IP address. The name of the property is `Proxy.OutboundIP`. Its value is the IP address in the list position determined by the property parameter.

**List of IP addresses for controlling outbound source IP addresses**

The list of IP addresses that you can use to replace outbound source IP addresses is part of the `Proxies` settings. You can find it there under `Advanced Outgoing Connection Settings`. Its name is `Outbound Source IP list`.

The following applies regarding the position of an IP address in the list:

- The list index starts from 0. If you specify, for example, 2, as the parameter of the `Proxy.OutboundIP` property to determine a position, the third IP address on the list is selected.

- If you specify a parameter value that is higher than the number of list entries, the position is determined by calculating `<parameter-value> modulo <number-of-list-entries>`.

  For example, if you specify 5 for a list that has only three list entries, the result of the modulo calculation is 2. The third IP address on the list is then selected.

**Network routing and IP address spoofing**

The IP addresses that are inserted into data packets by the `Enable Outbound Source IP Override` event are non-local source IP addresses. You must therefore configure network routing in a suitable way.

Data packets that are sent back from a web server to a client must be routed to the proxy on Web Gateway. You can, for example, use static routes to route the data packets.

When the `Enable Outbound Source IP Override` event is triggered and you have IP address spoofing enabled, the event also overrides this setting.

**Logging the use of outbound IP source addresses**

Several properties are available for logging data about outbound connections, including the source IP address and port that Web Gateway uses when connecting to web servers or next-hop proxies.

These properties are set to particular values, regardless of whether you have configured a single source IP address, using the `Enable Outbound Source IP Override` event. But you can also use them in this case.

- `Proxy.Outbound.IP` — Stores the source IP address that Web Gateway uses when connecting to web servers and next-hop proxies.

  Do not confuse this property with `Proxy.OutboundIP`, which has no dot before `IP` and is used together with the `Enable Outbound Source IP Override` event to select a single source IP address from a list.

- `Proxy.Outbound.Port` — Stores the source port that is used by Web Gateway when connecting to web servers or next-hop proxies.

- `Proxy.Outbound.IPList` — Stores the list of source IP addresses that Web Gateway can select an address from when connecting to web servers and next-hop proxies.

  The list is configured as part of the `Proxies` settings under `Advanced Outgoing Connection Settings`. Its name is `Outbound Source IP list`. When a single source IP address for outbound connections is configured, it is taken from this list.
Configure control of outbound source IP addresses
Replace different outbound source IP addresses with a single address to avoid connection problems.

Task
1. Select **Configuration** | **Appliances**.
2. Select an appliance for configuring the replacement of IP addresses, then select **Proxies (HTTP(S), FTP, SOCKS, ICAP ...)** and scroll down to **Advanced Outgoing Connection Settings**.
3. Under **Outbound source IP list**, add one or more IP addresses to the list of source IP addresses for outbound requests.
4. Add the following event to an existing rule for connections to web servers or next-hop proxies: **Enable Outbound Source IP Override with Proxy.OutboundIP property as a parameter**.

The rule now uses the list that you have configured to select an IP address for replacing different outbound source IP addresses.

Best practices - Configuring FTP over HTTP

Working with FTP over HTTP, users can retrieve files from an FTP server without setting up and configuring an FTP client.

FTP over HTTP is a type of HTTP traffic going on between a web browser and a proxy, such as the proxy provided by Web Gateway. In most respects, sending an FTP-over-HTTP request is like sending any other HTTP request. The difference is that the requested resource resides on an FTP server rather than an HTTP server. FTP over HTTP traffic is configured in explicit proxy mode.

An FTP-over-HTTP request contains a URL prefixed with `ftp://` instead of `http://`. The HTTP host header value includes port 21 instead of no port number (in which case port 80 is assumed).

The following is an example of an FTP-over-HTTP request that a client sends to Web Gateway at the beginning of the communication.

```plaintext
GET ftp://10.10.80.200/ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: 10.10.80.200:21
Proxy-Connection: Keep-Alive
```

When Web Gateway receives this request, it recognizes that the requested resource resides on an FTP server, due to the presence of `ftp://` and port 21.

Web Gateway then uses native FTP to retrieve the resource from the FTP server. Any FTP response traffic is "translated" on Web Gateway into HTTP terms before passing it on to the client. Sometimes this requires Web Gateway to create an HTML page, so the client can display the results, for example, a listing of FTP directories, in the web browser.

Use of the HTTP proxy port

FTP over HTTP is handled on Web Gateway much like any other HTTP communication with a client. Requests should therefore be sent from the client to the HTTP proxy port on Web Gateway, which is 9090 by default.

There is no need to configure the FTP proxy port, which is 2121 by default, as use of this port is only required if a client sends requests under the native FTP protocol.
Advantages and disadvantages

FTP over HTTP has advantages and disadvantages. Using this method to retrieve files from an FTP server allows users to work with a web browser, which saves them the effort of setting up and configuring an FTP client, such as the open-source Filezilla client.

The major disadvantage of FTP over HTTP is that it does not allow users to upload files. File upload requires the use of native FTP, an FTP client program on the client system, and use of the FTP proxy port on Web Gateway if users choose to send traffic this way.

Another disadvantage of FTP over HTTP is that most web browsers have issues with it.

Configure your own FTP credentials for anonymous logon

When a client sends an FTP-over-HTTP request that does not contain user credentials to Web Gateway, preconfigured credentials are used by default to perform anonymous logon to the FTP server. You can configure FTP credentials of your own to replace the default credentials.

Task
1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance that you want to configure FTP credentials on, then click Proxies.
3. Scroll down to HTTP Proxy and proceed as follows:
   a. Under Anonymous login for FTP over HTTP, type a user name.
   b. Under Password for anonymous login for FTP over HTTP, type a password.
4. Click Save Changes.

Troubleshooting browser issues arising for FTP over HTTP

Testing has shown that Mozilla Firefox is the only browser that does not require special attention from the user or administrator when doing FTP over HTTP.

Most web browsers have issues when requests are sent using FTP over HTTP. For some of these issues, you can implement workarounds.

Anonymous and non-anonymous logon

Some browsers can only handle FTP over HTTP when anonymous logon is allowed on an FTP server, as these browsers cannot send credentials as part of the URL in a request.

Other browsers prompt users for credentials when anonymous logon is not allowed on an FTP server.

When working with browsers that can handle non-anonymous logon, but do not prompt users, credentials can be submitted in one of the following ways:

- Credentials can be entered on the authentication page that is sent to the browser by Web Gateway.
- Credentials can be inserted in the URL that is sent from the browser to the FTP server. The URL format must be as follows:

  ftp://<user name>:<password>@<name of the FTP server>

Special characters within credentials

Some browsers do not encode FTP user names and passwords containing special characters correctly, rendering them useless and causing logon to fail.
There is no workaround for this issue, other than avoiding special characters in credentials. These browsers can be used, but are not recommended for FTP over HTTP when credentials for non-anonymous logon are required.

**Proxy authentication**

When doing FTP over HTTP using a proxy, for example, the proxy provided by Web Gateway, the proxy has to authenticate to the FTP server.

Some browsers cannot handle this authentication process. When Web Gateway sends a message that proxy authentication is required, these browsers do not send the user credentials back.

As a workaround, you can exempt these browsers from proxy authentication. For this exemption, a rule must be inserted in the rule set that you are using to control authentication. The rule recognizes the browser through the information provided by the user-agent information in the header of the request that is submitted.

This rule might look as follows if the browser is, for example, Google Chrome:

**Name**

Exempt FTP over HTTP with Chrome from proxy authentication

**Criteria**

Header.Get("User-Agent" matches "Chrome" AND URL.Protocol equals "ftp"

**Action**

Stop Rule Set

**Proxy settings**

Some browsers ignore the proxy settings when the protocol information in a URL is ftp://. Instead of sending an FTP over HTTP request to the proxy, they send a native FTP request directly to the FTP server.

There is no workaround for this issue. These browsers cannot be used for FTP over HTTP traffic.

**Issues with commonly used web browsers**

The following table shows issues that arise more often when doing FTP over HTTP in relation to some of the most commonly used web browsers.

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Issues</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>No issues known.</td>
<td>Can be used without taking additional measures for FTP over HTTP.</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>Does not prompt users for credentials when anonymous logon is not allowed for FTP over HTTP on an FTP server.</td>
<td>Can be used for FTP over HTTP when anonymous logon is allowed on an FTP server.</td>
</tr>
<tr>
<td></td>
<td>Encodes special characters within credentials incorrectly.</td>
<td>When user for non-anonymous logon, credentials must be submitted in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Entering credentials on the authentication page that is displayed by Web Gateway.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inserting credentials in the URL that is sent to the FTP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The credentials must not contain special characters.</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Can only handle FTP over HTTP if an FTP server allows anonymous logon.</td>
<td>Can be used if an FTP server allows anonymous logon, but requires a rule for skipping proxy authentication.</td>
</tr>
</tbody>
</table>
Table 4-1  Issues with web browsers when doing FTP over HTTP (continued)

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Issues</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opera</td>
<td>Cannot handle proxy authentication.</td>
<td>Can be used for FTP over HTTP, but requires a rule for skipping proxy authentication.</td>
</tr>
<tr>
<td>Safari</td>
<td>Ignores proxy settings when the protocol information in a URL is ftp://. Sends native FTP requests from a client directly to the FTP server instead, bypassing the configured proxy, for example, the proxy provided by Web Gateway.</td>
<td>No workaround: Cannot be used for FTP over HTTP.</td>
</tr>
</tbody>
</table>

Using WCCP to redirect FTP traffic

Requests that clients of Web Gateway send to servers under the FTP protocol can be redirected to Web Gateway using the WCCP (Web Cache Control Protocol) redirection method.

To send a request to a server under the FTP protocol, a client of Web Gateway opens the initial FTP connection. The client uses the IP address of the server for this connection. To let Web Gateway act as a proxy, the request is redirected to the IP address of the appliance that Web Gateway runs on.

Under the default settings, the client considers this redirection as a security risk and does therefore not continue with opening the FTP data connection. When redirection is performed using the WCCP protocol, you can solve this problem by modifying the settings as follows:

- Using the active FTP mode for the connection from the client to the proxy
  
  Clients are by default allowed to use the passive FTP mode. You can enforce the active FTP mode by disabling an option of the proxy settings on the user interface of Web Gateway.

- Configuring a port for redirection to the proxy
  
  This port must be entered in the list of ports that are redirected under WCCP.

- Letting the proxy use the IP address of the FTP server instead of its own IP address
  
  Setting a particular parameter ensures that the proxy uses this address.

After modifying the settings in this way, a client uses the active FTP mode. It sends the proxy an IP address and a port number to connect to. The proxy returns a synchronization message. In this message, the IP address of the FTP server is used as the source IP address of the proxy. The port number is 21 or 2020.

The client responds with the IP address of the FTP server as its destination IP address and the same port number. Requests from the client to the FTP server are then redirected to the proxy, using WCCP as the redirection method.

ℹ️ The WCCP redirection method cannot be used for FTP traffic in transparent bridge or router mode.
Configure the use of WCCP for redirecting FTP traffic

To enable the use of the WCCP redirection method for requests that clients send to servers under the FTP protocol, configure the proxy settings as follows.

**Task**

1. **Enforce use of the active FTP mode by clients.**
   
   a. Select **Configuration** | **Appliances**.
   
   b. On the appliances tree, select the appliance that you want to enable use of the WCCP redirection method for, then click **Proxies (HTTP(S), FTP, SOCKS, ICAP ...)**.
   
   c. Scroll down to **FTP Proxy** and make sure that **Enable FTP proxy** is selected.
   
   d. Select an entry in the **FTP port definition list**, click **Edit**, and under **FTP Proxy Port**, deselect **Allow clients to use passive connections**.
      
      Repeat this substep for all entries in the list.

2. **Add ports 21 and 2020 to the ports that are used for redirection under WCCP.**
   
   a. Within the **Proxies** settings, scroll to **Transparent Proxy**, and under **Supported redirection methods**, make sure that **WCCP** is selected.
   
   b. Select an entry in the **WCCP services list**, click **Edit**, and under **Ports to be redirected**, type **21,2020**.
      
      Repeat this substep for all entries in the list.

3. **Click **Save Changes**.**

4. Within the relevant settings, set the **ftp.match.client.data** parameter to **yes**.

   This setting ensures that Web Gateway uses the IP address that it received from the client as its source IP address when responding to the client.

   This address is the IP address of the FTP server in question, not the IP address of the Web Gateway appliance. The client does therefore not suspect a security risk.

Requests sent from a client to a server under the FTP protocol are now redirected to Web Gateway, using the WCCP redirection method, and processed without problems.

**Using the Raptor syntax for FTP logon**

When Web Gateway is configured to run as an FTP proxy, the Raptor syntax can be used for logging on to an FTP server with Web Gateway as a proxy.

To perform this logon, the user who wants to access the FTP server can run the USER, PASS, and ACCEPT commands from a suitable FTP client. Using these commands, the FTP server is specified together with user names and passwords for both the FTP server and the Web Gateway proxy.

The command syntax is as follows:

- **USER** `<ftpuser>@<ftpserver> <proxyuser>`
- **PASS** `<ftplusertpass>`
- **ACCT** `<proxyuserpass>`

The following table describes the meanings of the command parameters.
Table 4-2  Command parameter for FTP logon

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftpserver</td>
<td>FTP server that access is requested to</td>
</tr>
<tr>
<td>ftpuser</td>
<td>User name on the FTP server</td>
</tr>
<tr>
<td>ftpuserpass</td>
<td>Password for the FTP server</td>
</tr>
<tr>
<td>proxyuser</td>
<td>User name on the Web Gateway proxy</td>
</tr>
<tr>
<td>proxyuserpass</td>
<td>Password for the Web Gateway proxy</td>
</tr>
</tbody>
</table>

Node communication protocols

When Web Gateway appliances run as director and scanning nodes in a Central Management configuration, communication between the nodes uses the Virtual Router Redundancy Protocol (VRRP) and MWG Management Protocol.

Use of the protocols depends on the proxy settings that you have configured on the appliances that run as nodes. The protocols differ with regard to the activities of director and scanning nodes that are covered by them.

**Virtual Router Redundancy Protocol**

The Virtual Router Redundancy Protocol is used when you have configured Web Gateway as a proxy in transparent router mode or High Availability proxy mode.

Under this protocol, virtual IP addresses are assigned to active director nodes and backup director nodes. The protocol also determines which director node takes the active director role.

**MWG Management Protocol**

The MWG Management Protocol is used in transparent router, transparent bridge, and High Availability proxy mode. Under this protocol, scanning nodes are identified as available for processing web traffic.

The node that takes the active director role sends out broadcast messages to the scanning nodes, using the IP address that you have configured as its source IP address under the Management IP option of the respective proxy settings.

The protocol lets scanning nodes that are available within the same network segment respond in regular intervals to the discovery messages of the director node.

**Security considerations**

The security features of the Virtual Router Redundancy Protocol and MWG Management Protocol are similar to that of the Address Resolution Protocol (ARP).

The Virtual Router Redundancy Protocol uses multicast with an IP address that is not routed beyond the local broadcast domain. MWG Management Protocol uses broadcast messages.

A malicious node on the same network segment might send VRRP messages and hence impersonate itself as the active director node holding the respective virtual IP address. If that node decides to drop all data packets it receives for the virtual IP address, network connectivity stops for the clients that are connected to Web Gateway.

**Best practice:** Use IP addresses from a protected network segment when configuring proxy settings according to the Virtual Router Redundancy Protocol and the MWG Management Protocol. This will prevent malicious nodes from impacting Web Gateway activities.
Using DNS servers according to domains

The use of DNS (Domain Name System) servers to resolve domain information provided in URLs into IP addresses when requests for web access are processed on Web Gateway can be configured according to the domains of the requested destinations.

This use of DNS servers is also known as conditional DNS forwarding.

Domains, for example, testnet.webwasher.com, are entered into a list together with the IP address of the DNS server that is used to resolve the URL information. More than one DNS server can be specified this way for a domain.

When a request to a particular destination on the web is sent to Web Gateway, it is forwarded to a DNS server according to this list.

The use of a particular DNS server can be configured dynamically with DHCP (Dynamic Host Configuration Protocol). This is also the default setting after the initial setup of a Web Gateway appliance.

If both configuration with DHCP and conditional DNS forwarding are configured, DHCP takes precedence and conditional DNS forwarding is bypassed.

If a BIND server is configured as a DNS server, the DNS server settings that are stored in a configuration file on Web Gateway will be overwritten. To keep these settings for domain name resolving, you need to enter them manually again.

Configure the use of DNS servers according to domains

To enable the use of DNS servers according to the domains of destinations in the web, configure the Domain Name Service settings in a suitable manner.

Task

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to configure the use of DNS servers for and click Domain Name Service.
3. Configure the settings in the Conditional DNS Forwarder Configuration section as needed.
4. Click Save Changes.

Using DXL messages to exchange web security information

You can use the DXL technology to send and receive information to and from web security products that are connected to Web Gateway in a common security architecture.

McAfee® Data Exchange Layer (DXL) is a messaging technology for real-time information exchange. The technology is used to exchange security-related information, for example, file reputation scores between Web Gateway and other web security products that are connected to it.

This kind of information exchange is part of a security architecture that is provided by McAfee and is also known as Security Connected.

Scenarios for exchanging web security information

You can exchange information under DXL in two main scenarios: One is publishing a message about a security topic in an event and receiving this message after subscribing for the topic. The other is sending a query for information about a security topic to a service and receiving a response from this service.
The web security products that are connected to each other, including Web Gateway, take the various roles that belong to these scenarios. Products can be publishers and subscribers, they can send queries and also act as services that queries are sent to.

When a publisher sends DXL messages to the subscribers, they send no responses. When a DXL message is sent as a query for security-related information to a service, the service sends a response, providing information about the topic that was specified in the query.

Web Gateway supports the sending of DXL messages in events and as queries to a service. It can also receive DXL messages and act as a service that provides information about a web security topic.

You can implement the Gateway Anti-Malware with TIE library rule set that uses DXL messages to exchange file reputation information between Web Gateway and a TIE server. This is the only way to use DXL messages on Web Gateway.

**Configuring settings for the exchange of web security information**

When information about web security topics is exchanged on Web Gateway, several settings are involved. These settings include credentials for a McAfee ePO server, as parts of the DXL architecture are managed by this administration product.

Topics and services for information exchange are part of the settings for the proxy functions of Web Gateway.

DXML messages can also be traced for troubleshooting after enabling the relevant option of the Troubleshooting settings.

**Best practices - Working with the user-agent header**

The user-agent header is a header in a request for web access sent under the HTTP protocol. This header identifies the software program that was used to send the request. You can work with this header to create a rule that performs a particular action on a request that contains this header.

The software used on a client for sending a request can be a browser, a media player, or a similar program. If you find, for example, that requests sent with a particular browser cause issues with user authentication on Web Gateway, you can create a rule that skips authentication for these requests or blocks them.

The rule contains the value of the user-agent header in the criteria for the action that is performed. When a request is processed on Web Gateway, this value is retrieved from the request to see whether it is the one for the software program that causes issues.

If not only one program causes issues or you expect that more will be found, you can also work with a list of user-agents. The value of the user-agent header within a request is then compared to the list entries to see whether it matches any of them.
Finding the user-agent

To create a rule with an action for a request that caused issues due to its user-agent, you must know which user-agent it is. There are several ways to find this out.

- **Access log** — You can inspect the access log that is maintained on Web Gateway. The data that this log records includes the user-agent header of a request by default.

- **Online resources** — You can find information about browsers, media players, and similar programs that run as user-agents on client systems using online resources, for example, performing an online search. Websites are available that support your search for information, for example, by listing and describing the most common user-agents or by identifying the browser that is currently in use on a client.

- **TCP dump** — You can create a TCP dump of the request processing that Web Gateway performs, using the troubleshooting functions on the user interface. For more information about these functions, see the Troubleshooting chapter.

When a TCP dump has been created, you can work with a packet tracing tool, for example, Wireshark, to follow the TCP stream. You can select a GET request sent for web access and inspect the data packets of this request with its headers.

If you already have some information about the user-agent that causes issues, you can filter the output in Wireshark accordingly. Entering, for example, the following line returns all data packets that contain the text string "Mozilla".

```
http.user_agent matches "Mozilla"
```

Most user-agent headers for browsers begin with the text string "Mozilla". This does not necessarily mean that the user-agent is the Mozilla Firefox browser. It could be Firefox or a different browser.

Common user-agent headers

The following list provides information about some user-agent headers for software programs that are often found when TCP dumps created on Web Gateway are inspected.

Codes lines from the Wireshark packet tracing tool showing the relevant information are added for each user-agent header.

- **Firefox** — A user-agent header for a Mozilla Firefox browser contains the text string "Firefox/" followed by the version number.

  ```
  Mozilla/6.0 (Windows NT 6.2; WOW64; rv:16.0.1) Gecko/20121011 Firefox/16.0.1
  ```

- **Internet Explorer** — A user-agent header for a Microsoft Internet Explorer browser contains the text string "MSIE" followed by the version number.

  ```
  Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
  ```

- **Chrome** — A user-agent header for a Google Chrome browser contains the text string "AppleWebKit".

  ```
  Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.172 Safari/537.22
  ```

Do not confuse a header like this with a user-agent header for the Apple iPhone smartphone.
Windows Media Player — A user-agent header for Windows Media Player contains the two text strings shown in this sample code block.

```
Windows-Media-Player/10.0.0.xxxx
NSPlayer/10.0.0.xxxx WMFSDK/10.0
```

iTunes — A user-agent header for an Apple iTunes media player contains the text string "iTunes/" followed by the version number.

```
Mozilla/6.0 (Windows NT 6.2; WOW64; rv:16.0.1) Gecko/20121011 Firefox/16.0.1
```

Safari on iPhone — A user-agent header for an app that runs on an iPhone, for example, the Apple Safari browser, contains the text string "iPhone".

```
Mozilla/6.0 (Windows NT 6.2; WOW64; rv:16.0.1) Gecko/20121011 Firefox/16.0.1
```

**Sample rule for working with the user-agent header**

In a rule that performs an action on a request with a user-agent header for a particular software program, the user-agent is included in the rule criteria. If the rule is to apply for more than one user-agent, you can work with a list of user-agents.

We recommend using a list, even if you are presently interested in a particular user-agent only. Using a list makes it easier to modify the rule when more user-agents must be addressed in the future.

The rule criteria contains a property that is set to the value for the user-agent in the user-agent header when the rule is processed. The rule applies if this value matches one of the entries in a list of user-agents or a single user-agent if you have configured the rule this way.

The list might, for example, contain the entry "MSIE 10" for version 10 of the Microsoft Internet Explorer. If a request includes a user-agent header for this browser, the rule criteria matches, as the string that you entered in the list is also contained in the user-agent header.

The property that is used to retrieve the value for the user-agent from the user-agent header in a request is `Header.Request.Get`. To use the property for retrieving this value, you configure the string "User-Agent" as a parameter of the property.

The purpose of the sample rule is to let a request skip SSL scanning. It looks as follows.

Name  
Skip SSL Scanner for user-agents in list

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Header.Request.Get(&quot;User-Agent&quot;) matches in list User Agent Whitelist</code></td>
<td><code>Stop Rule Set</code></td>
</tr>
</tbody>
</table>

We recommend including still another criteria part in a rule like this. As it is the client that provides the information about the user-agent, the client or a malware program might spoof a trusted user-agent to bypass filtering.

A sample rule that has its criteria extended by another part to protect the rule against user-agent spoofing looks as follows.

Name  
Skip SSL Scanner for user-agents in list

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Header.Request.Get(&quot;User-Agent&quot;) matches in list User Agent Whitelist</code></td>
<td><code>Stop Rule Set</code></td>
</tr>
</tbody>
</table>

We recommend including still another criteria part in a rule like this. As it is the client that provides the information about the user-agent, the client or a malware program might spoof a trusted user-agent to bypass filtering.
In the sample rules, **Stop Rule Set** is configured as action. To address issues that a user-agent causes with regard to a function of Web Gateway, you insert the rule in the rule set for that function.

For example, if a user-agent causes issues with SSL scanning, insert it at the beginning of the **SSL Scanner** rule set. If the rule applies, processing of this rule set is stopped, which means that the relevant request skips SSL scanning. The rule can be used in a similar way to skip, for example, user authentication.

If you do not want to let requests skip anything due to issues with user-agents, you can replace the **Stop Rule Set** action with **Block**. You can then create a rule set for globally blocking requests (if it does not yet exist in your rule set system) and insert the rule.

## Create a rule for working with the user-agent header

Create a rule that performs an action on requests depending on their user-agent headers to address issues caused by the user-agents.

The following procedure assumes that an issue with SSL scanning is caused by a particular user-agent. The rule that is created lets requests with user-agent headers containing this user-agent skip SSL scanning to avoid the issues.

### Task

1. Select the rule set for the function that is skipped for requests with the user-agent that causes issues.
   
   a. Select **Policy | Rule Sets**.
   
   b. On the rules tree, select the **SSL Scanner** rule set.
   
   c. Click **Unlock View** on the configuration pane and confirm with **Yes**.

   The nesting **SSL Scanner** rule set is accessible for inserting rules.

2. Configure the name of the rule that lets requests skip the rules in the rule set.
   
   a. Click **Add Rule**.

   The **Add Rule** window opens with the **Name** step selected.

   b. In the **Name** field, type a name for the rule, for example, **Skip SSL Scanner for user-agents on list**.

3. Configure the property that is used to retrieve the user-agent.
   
   a. Click **Rule Criteria** and then **Add**.

   b. From the drop-down menu, select **Advanced Criteria**.

   The **Add Criteria** window opens.

   c. Click **Filter**, then select **Engine | Header** and from the filtered list of properties select **Header.Request.Get**.

   d. Click **Parameters** at the property.

   e. In the window that opens, make sure that **Parameter value** is selected and type **User-Agent**, then click **OK** to close the window.
4 Configure the operator and the list to compare the property value with.
   a Leave the Matches in list operator that is suggested.
   b From the lists under Compare with, select User Agent Whitelist.
      
      The list is initially empty and you must insert an entry for the user-agent that causes issues.

   c Click OK.

      The Add Criteria window closes and the complete criteria appears in the Add Rule window.

5 Configure the rule action.
   a Click Action.
   b From the Action list select Stop Rule Set

6 Complete the configuration.
   a Click Finish.

      The Add Rule window closes and the rule appears in the SSL Scanner rule set.

   b Click Save Changes.

---

**Bypassing for Office 365 and other Microsoft services**

Requests sent to Office 365 and other Microsoft services, and responses received from these services, can be configured to bypass filtering to avoid a load increase on Web Gateway.

Bypassing is handled for these requests and responses by rules. A rule set with suitable rules is provided in the default rule set system and in the rule set library.

To configure the bypassing of requests and responses in traffic to and from Office 365 and other Microsoft services, you can work with:

- **Key elements of rules** — After opening the rule set with the bypassing rules, you can view and configure key elements of these rules.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the bypassing rules completely, configure all their elements, including the key elements, and also create rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or reimport the rule set.

---

**Office 365 and other Microsoft services**

Microsoft offers several cloud-based applications that belong to the Office 365 application suite. These applications rely heavily on HTML5 features to provide an enriched user experience.
Consequently, some of these applications can set up a high number of connections and also several "endless" connections, which might considerably increase the load on a Web Gateway appliance. The increased load can have an impact on the proxy functions of Web Gateway, leading to slow or delayed web access, timeouts, and other issues.

To avoid such issues, you might want to let requests and responses in traffic to and from Office 365 and other Microsoft services bypass filtering on Web Gateway. Many of these requests and responses also use undocumented formats or protocols that are proprietary to Microsoft and cannot be scanned and filtered on Web Gateway.

**Rule set for Microsoft services bypassing**

The Bypass Microsoft (Office 365) Services rule set contains rules that enable bypassing for requests and responses in traffic to and from Office 365 and other Microsoft services.

IP address and URL lists published by Microsoft are used to recognize the requests that are submitted for accessing these services.

The rule set is placed at the top of the default rule set system.

**Using a Domain Name System**

The bypassing rule set requires Web Gateway to access a Domain Name System (DNS). In some configurations, for example when next-hop proxies are used, Web Gateway does not normally require DNS access, so this access might not be configured or even be blocked by a rule.

Most of the rules in the rule set, however, rely on evaluating the URL.Destination.IP property to recognize relevant requests. The DNS is then used to resolve the destination IP address of the request that is currently processed.

So, if a DNS is not correctly configured or not configured at all, you might encounter timeouts or slow performance when working with the rule set.

**Key elements for Microsoft services bypassing**

The key elements of the rules that handle bypassing for Office 365 and other Microsoft services are related to the individual services that requests and responses are sent to and received from.

**Bypassing for Microsoft services**

Options for handling Microsoft services bypassing

**Table 4-3 Bypassing for Microsoft services**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
Bypass Microsoft (Office 365) Services rule set

The Bypass Microsoft (Office 365) Services rule set is the default rule set for letting requests and responses in traffic to and from Office 365 and other Microsoft services bypass filtering on Web Gateway.

**Default rule set – Bypass Microsoft (Office 365) Services**

<table>
<thead>
<tr>
<th>Criteria – Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles – Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**Shortcut Microsoft service in response**

**Cycle.Name equals "Response" AND User-Defined.Shortcut_Microsoft_Service equals true – Stop Cycle**

The rule uses the **Cycle.Name** property to find out whether processing on Web Gateway is currently going on in the response cycle.

It also uses a user-defined property to check whether the response that is processed in this cycle was triggered by a client requesting access to Office 365 or any of several other Microsoft services.

If such a request is received on Web Gateway, a particular rule that is processed in the request cycle sets the user-defined property to **true**. The current rule checks whether the property is actually set this way in the response cycle, using the second part of its criteria.

If both criteria parts match, the rule applies and the response cycle is stopped. The response is then forwarded to the requesting client without filtering.

This rule is enabled by default.

All rules that follow the first rule in the rule set work in a similar way. They ensure that a request sent by a client of Web Gateway to a particular Microsoft service is forwarded to this service unfiltered.

Each of them also sets the property that is evaluated by the first rule to **true** after receiving such a request.

The first of these subsequent rules is explained here as an example in full detail. A summary is then given for all other rules.

**Bypass Exchange Online**

**URL.Destination.IP is in range list Exchange Online IP Addresses OR URL.Destination.IP is in range list Exchange Online Protection P Addresses OR URL.Host matches in list Exchange Online URLs – Stop Cycle – Set User-Defined.Shortcut_Microsoft_Service = true**

The rule uses the **URL.Destination.IP** and **URL.Host** properties to find out whether the IP address and URL that are sent with a request are on particular lists.

If they are, the request cycle is stopped and the request is forwarded to the requested destination, which is the Microsoft Exchange Online service.

The **User-Defined.Shortcut_Microsoft_Service** property is then set to **true** by an event. The property is evaluated in the response cycle by the first rule in the rule set.

This rule is not enabled by default.

**Bypass Microsoft Federation Gateway, Bypass Microsoft Lync/Skype for Business Online, and other rules for Microsoft services bypassing**

Similar to the **Bypass Exchange Online** rule, these rules use the **URL.Destination.IP** property or the **URL.Host** property or both (in one case also the **URL** property) to find out whether the IP addresses or URLs that are sent with requests are on particular lists. The lists vary with each rule depending on the respective service.

If the IP addresses or URLs are found on the lists, the request cycle is stopped and the request is forwarded to the requested destination, which is one of the Microsoft services.
The User-DefinedShortcut_Microsoft_Service property is then set to true by an event. The property is evaluated in the response cycle by the first rule in the rule set. None of these rules is enabled by default.

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
     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 addresses 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 an appliance for listening 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.
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 81*
  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 82*
  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.
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
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 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 83**
  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 83**
  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 84**
  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 87**
  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 84*
  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 85*
  You can create a rule set for the rule that blocks access to web servers in a reverse HTTPS proxy configuration.

- *Create a rule to block access to web servers on page 86*
  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**.
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**.

Enter one or more wildcard expressions matching the URLs for the web servers you want to protect. Separate multiple entries by commas.

Click **OK**.

The window closes and the new entries appear on the list.

Click **Save Changes**.

**Create a rule set for a blocking rule**

You can create a rule set for the rule that 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:
   - From the list of properties in the left column, select URL.Host.
   - From the list of operators in the middle column, select matches in list.
   - 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 list that appears, select Event.
   The Add Event window opens.
10 Configure an event as follows:
   - From the Event list, select Enable Proxy Control.
   - 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 87
  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 88
  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 88
  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.
Enter one or more wildcard expressions matching URLs for the web servers you want to address. Separate multiple entries by commas.

Click OK.

The window closes and the new entries appear on the list.

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 list 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.
Proxies
Using the Helix proxy
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 connected 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
- Configure Central Management
- Add an appliance to a Central Management configuration
- Assign a node to node groups
- Best practices - Configuring Central Management node groups
- Verify the synchronization of nodes
- Replace the cluster certificate
- Create a tenant ID
- Add a scheduled job
- Update the appliance software in a Central Management configuration
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.

When configuring appliances as nodes, you must make sure that they can connect to ("see") each other. The default port on an appliance that listens to messages from other appliances is 12346.

Using the ping command is a method to verify that appliances can connect. This method is, however, not applicable to all networks.

- There are different types of node groups that allow different kinds of data transfer between the group members.

A Central Management configuration of multiple Web Gateway appliances is often referred to as a cluster.

This does not mean, however, that it is necessarily a High Availability cluster with fail-over functions. It is this type of a cluster only if you configure the Proxy HA (High Availability) mode for the proxy functions of the appliances that are involved.

The following diagram shows several appliances that run as nodes in a Central Management configuration.

![Central Management configuration diagram](image-url)
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 nodes 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.

Secure cluster communication

Communication between the nodes in a Central Management cluster is usually SSL-secured. A default cluster certificate for this communication is included in the initial setup of Web Gateway.

**Best practice:** Replace the default cluster certificate with a certificate that you have created on your own using the options provided in the user interface.

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  *(Optional)* Replace the default certificate for SSL-secured communication between nodes with a certificate of your own.

3  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 in the configuration on the user interface of any other node in this configuration.

  **Best practice:** Do not change the default **Advanced Management Settings** unless necessary. If you change these settings, make sure that the **Use unencrypted communication** setting is the same for all nodes in the configuration.

- Add one or more new nodes to the configuration

4  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 now a node in a Central Management configuration with the appliance you have been working on to complete the addition.

**Tasks**

- **Import a cluster CA and its private key on page 97**
  Import a cluster CA and its private key to a Web Gateway appliance for signing the certificate that is generated to ensure secure communication between this appliance and other appliances that are nodes in a Central Management cluster.

- **Generate a cluster CA and its private key on page 98**
  Generate a cluster CA and its private key for use in generating certificates and private keys to ensure secure communication between Web Gateway appliances that are nodes in a Central Management cluster.

**Import a cluster CA and its private key**

Import a cluster CA and its private key to a Web Gateway appliance for signing the certificate that is generated to ensure secure communication between this appliance and other appliances that are nodes in a Central Management cluster.

**Task**

1 On the user interface of an appliance, select **Configuration | Appliances**.

2 At the top of the configuration pane, click **Cluster CA**.

3 In the **Cluster CA** window that opens, click **Change CA**.

4 Use the **Import Certificate Authority for Cluster** to import the cluster CA and its private key.
   - Browse to the location where you stored the cluster CA after generating it, then browse to the location where you stored its private key.
     - **This cluster CA must be used for signing the certificates of all appliances that are added as nodes to the cluster.**
   - Enter a password for the private key.
   - Click **Import**.

The cluster CA is imported with its private key. The private key enables use of the cluster CA, which then signs the certificate that is created on the appliance.

Together with this certificate, another private key is generated for enabling its use in secure cluster communication, and both items are stored on the appliance.

- **The private key of the Cluster CA is required for enabling its use in completing these activities, but it is not stored on the appliance.**

5 Click **Save Changes**.
**Generate a cluster CA and its private key**

Generate a cluster CA and its private key for use in generating certificates and private keys to ensure secure communication between Web Gateway appliances that are nodes in a Central Management cluster.

A cluster CA and its private key are first generated on a single appliance when you begin to create a cluster. More appliances can then be added to the cluster, after importing this cluster CA and its private key to each of them.

If you have already created a cluster and want to replace the cluster CA and the private key that are in use within this cluster, you can generate these items on any of the appliances that are its nodes.

Importing the cluster CA and its private key to other appliances is not required in this case, as certificates and private keys for all appliances in the cluster are generated when a cluster CA and its private key are generated on any of them.

**Task**

1. On the user interface of an appliance, select **Configuration | Appliances**.

2. At the top of the configuration pane, click **Cluster CA**.

3. In the **Cluster CA** window that opens, click **Generate CA**.

4. Use the **Generate Cluster CA Certificate** window that opens to generate a cluster CA and its private key.
   
   a. Under **Common Name**, type a common name for the cluster CA.

      If a cluster CA already exists on the appliance, its name is displayed here, together with the hash value of the name.

      The remaining fields in the window are grayed out, as filling them out is not required.

      The validity period for the cluster CA is set to 15 years. The RSA key size is set to 3072.

   b. Click **Apply and Export**.

      A cluster CA and its private key are generated. The private key enables use of the cluster CA, which then signs the certificate that is generated on the appliance that you are currently working on.

      Together with this certificate, another private key is generated for enabling its use in cluster communication, and both items are stored on the appliance.

      If you are generating the cluster CA and its private key on an appliance that is a node in an already existing cluster, certificates and private keys for all nodes in this cluster are also generated and stored.

      The **Generate Cluster CA Certificate** window closes and the **Save CA Certificate and Private Key** window opens.

5. Use the **Save CA Certificate and Private Key** window to store the cluster CA and its private key.

   It is mandatory that you complete this step here, as no opportunity will be provided to store these items later on.

   a. Next to **Exported CA certificate location**, click **Browse** and browse a location to store the cluster CA there.

   b. Next to **Exported private key location**, click **Browse** and browse to a location to store the private key there.

   c. Under **Encryption password**, type a password for the private key and hit the Enter key on your keyboard.

      The window closes and the cluster CA is stored with its private key.

   d. When a message informs you that both have been stored, click **OK** to close the message window.
A cluster CA and its private key have been generated and are stored in the places that you selected. The cluster CA is also stored on the appliance, but not its private key.

This private key was required, however, to enable use of the cluster CA when it signed the certificate that was generated on the appliance.

Be aware that this private key will again be required to enable use of the cluster CA when it is imported with the private key to sign a certificate for another appliance that is added as a node to the cluster.

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 99
  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 100
  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 100
  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 **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**.

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.

**Best practices - Configuring Central Management node groups**

In a Central Management configuration, nodes are assigned to node groups to enable different ways of communication between the nodes.

Node groups can also include nodes that are installed in different physical locations.

Before you begin to configure these groups, make sure the following applies:

- Appropriate routes are configured in your network to allow communication between nodes.
  - If nodes in different locations are protected by firewalls, they must allow use of the port that is configured on each node for communication with other nodes (default port: 12346).
- Time is synchronized. Node communication depends on this when it is determined which node has the most up-to-date configuration.

We highly recommend that you configure the use of an NTP server on each node for automatic synchronization. This is done as part of configuring the Date and Time settings of the Configuration top-level menu.

If you are not using an NTP server for your network, you can configure the default server that is provided by McAfee at ntp.webwasher.com.

- The same version and build of Web Gateway is running on all appliances that are configured as nodes.

**Small sample configuration**

In this sample configuration, there are two different locations (Tokyo and New York) with two nodes each. In both locations, the nodes are assigned to their own runtime, update, and network groups. The group names are tokyo and newyork, respectively, for all types of groups.

One node in each location is also assigned to the transit network group, which is the same for both locations.

The following diagram shows this configuration.
This way, the following is achieved:

• Policy changes that an administrator configures on any node are distributed to all other nodes, due to the existence of a transit group node in each location. This ensures the web security policy remains the same on all nodes.

The changes are transferred, for example, from the non-transit node in New York to the transit node because both are in one network group. They are then transferred from this transit node to the node in Tokyo, again, because both are in one network group, the transit group.

Finally, the changes are transferred from the Tokyo transit node to the other node in this location.

• Updates of anti-malware and URL filtering information for the respective modules (engines) of Web Gateway are only distributed between nodes in Tokyo and between nodes in New York.

This allows you to account for differences in the network structure of locations, which is advisable regarding the download of potentially large update files.

Nodes in one location with, for example, fast connections and LAN links can share these updates, while they are not distributed between these nodes and those in other locations with, for example, slower connections and WAN links.

> We generally recommend that you include only nodes of one location in the same update group.

• Runtime data, for example, the quota time consumed by users, is only distributed between nodes in Tokyo and between nodes in New York.

This makes sense, as probably users in one location will only be directed to the local nodes when requesting web access. So it would not be required for a node in New York to be informed about, for example, the remaining quota time of a user in Tokyo.

> If the nodes in one location are assigned to different user groups with regard to their web access, you can also configure these nodes in different runtime groups to avoid an information overhead on any node.

Larger sample configuration

Not more than 10 nodes should be configured for a network group together with a transit node. This means that in larger locations, you need to configure more than one node for the transit network group.

In the following sample configuration, there are 22 nodes in one location (Tokyo), which are split into two network groups (toknet1 and toknet2), both of which include one node that is also a member of the transit group.

The 18 nodes in the second location (New York) are configured in the same way, whereas the 9 nodes in the third location (Paderborn) are all in one network group with one node that is also in the transit group.
The following diagram shows this configuration.

Regarding runtime and update node groups, there is one of each type for every location.
Policy changes, updates of anti-malware and URL filtering information, as well as sharing of runtime data are handled in the same way as for the smaller sample configuration.

**Alternative configuration of nodes with transit group functions**

You can configure nodes that perform the functions of nodes in a transit group without formally creating a transit group as a group of its own.

If you have, for example, two groups of nodes, each of which is configured as a network group, you can configure one of the nodes in each group to be a member not only of its own, but also of the other network group.

The nodes that are configured in this way will perform transit group functions. For example, they will distribute policy changes that the administrator applies on one node to all other nodes in the two groups.

**Best practice:** For smaller node groups, configure one node as a member of its own group and of the other group or groups. For larger node groups, configure more than one node with multiple membership for every node group.
Verify the synchronization of nodes

The user interface displays, among other general information, a timestamp for each node in a Central Management Configuration, which allows you to verify whether all nodes are synchronized.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select **Appliances (Cluster)**.
   
   Status and general information about the configuration and its nodes appears on the settings pane.

   Under **Appliances Information**, a list is shown that contains a line with information for every node. The timestamp is the last item in each line.

3. Compare the timestamps for all nodes.
   
   If they are they same for all nodes, the Central Management configuration is synchronized.

Replace the cluster certificate

To replace the default certificate for SSL-secured communication between cluster nodes with a certificate of your own, generate a certificate and import it into the cluster.

**Create a cluster certificate**

Create settings for your own cluster certificate and generate it as using the options of these settings.

**Task**

1. On the user interface of an appliance that is a node in the cluster, select **Policy** | **Settings**.
2. On the settings tree, navigate to **SSL Client Context with CA**.
3. Create settings for the certificate.
   a. On the settings toolbar, click **Add**.
   b. In the **Name** field, type a suitable settings name, for example, **Own Cluster Certificate**.
   c. (Optional) In the **Comment** field, type a plain-text comment on the settings.
   d. Click **OK**.
      
      The new settings appear on the settings tree.
4. Select the new settings.
   
   Settings parameters with default values appear on the configuration pane under **Define SSL Client Context (Certificate Authority)**.
5. Generate a certificate of your own.
   a. Click **Generate**.
   b. Enter appropriate values in the various fields of the window, then click **OK**.
      
      A certificate with your values is generated. The window closes and the certificate values appear under **Define SSL Client Context (Certificate Authority)**.
      
      A private key for the certificate is also generated and ready for exporting.
6  Export the certificate to make it available for distribution within the cluster.
   a  Click Export.
      Your local file manager opens.
   b  Browse to where you want to export the certificate to. In the File Name field, type a name for the certificate file, with a .cer or .crt ending as needed, then click Save.
      The certificate is exported to the selected location.

7  Export the private key for the certificate.
   a  Click Export Key.
      The Save Private Key window opens.
   b  Click Browse.
      Your local file manager opens.
   c  Browse to where you want to export the private key to. In the File Name field, type the file name that you used for the certificate, then click Save.
      The .pem file name extension, is supplied by the export process.
      The path to the private key appears in the Exported private key location field of the Save Private Key window.
   d  (Optional) For enhanced security, type a password for the key in the Password field.
   e  Click OK.
      The private key is exported to the selected location.

Distribute a certificate in the cluster
To distribute a certificate of your own in the cluster, import it onto one of the cluster nodes. The cluster distribution process then transfers the certificate to all other nodes.

Task
1  Select Configuration | Appliances.
2  On the appliances tree, select Appliances, then click Cluster CA on the configuration pane.
3  Click Change CA .
   The Import Certificate Authority for Cluster window opens.
4  Import a cluster certificate of your own.
   a  Next to Certificate, click Browse.
      The local file manager opens.
   b  Browse to the file with your own certificate and click Open.
      The path to the certificate file appears in the Certificate field of the Import Certificate Authority for Cluster window.
   c  Next to Private Key, click Browse. Browse to the file with the private key and click Open.
   d  If you created a password for the key, type it in the Password field.
   e  Click Import.
The window closes and the certificate is imported to the node that you are presently working on. The cluster distribution process transfers the certificate to all other nodes.

Create a tenant ID

Create a tenant ID, which identifies you as the owner of this instance of Web Gateway and of other Intel security products that you have purchased.

To create the tenant ID, you work with the options of the user interface and with McAfee ePolicy Orchestrator Cloud (McAfee ePO Cloud).

![A valid license must have been activated to enable creation of a tenant ID.](image)

**Task**

1. Select *Configuration* | *Appliances*.
2. On the appliances tree, expand *Cluster*, then click *Tenant Info*.
   
   The **Tenant Info** settings appear in the configuration pane.
3. Click **Show Provisioning Key**.
   
   The key is generated based on your customer ID and the current time stamp using SHA256 and base64 encoding. When the key has been generated, it is displayed in the field below the button.
4. Click **Copy** to copy it for use with McAfee ePO.
5. Create an activation key for the tenant ID, working with McAfee ePO.
   
   For more information, see the documentation for this product.
6. After creating the activation key with McAfee ePO, copy it and paste it into the lower input field of the **Tenant Info** settings.
7. Click **Set Tenant ID** to generate the tenant ID.
   
   The tenant ID is made known on this appliance and all others that are nodes in the same cluster.
8. Click **Save Changes**.

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.

---

**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:

   ```bash
   yum install yumconf-<version number>-mwg
   ```

   *yumconf-<version number>-mwg* is the repository name. The digits of the version number must be separated by dots.

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 Update each appliance on the appliances tree, except the appliance you are working from.
   a On the appliances tree, select an appliance.
   b On the toolbar above the settings pane, click **Update appliance software**.
When all other appliances that are nodes in the configuration are running their updates, perform the update for the appliance you are working from.

- Select the appliance on the appliances tree.
- 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 appliance software is now updated.
Policy configuration

To protect your network against threats arising from the web, Web Gateway enforces a web security policy, which is implemented during the initial setup. You can configure this policy later on to adapt it to the needs of your organization.

When performing this configuration, you will be dealing with several concepts and processes.

• **Web security policy** — A web security policy is made up of rules, which are grouped in rule sets on Web Gateway.

  When a situation arises where a rule applies, it performs an action to handle this situation. The situation can be an immediate threat, for example, a virus in a file that a user who works within your network attempts to download. In this case, the rule would block the attempt.

  Other situations might be that a user requests access to an online shopping site during work hours or tries to download a very large streaming file. Both activities could be blocked by suitable rules.

  You can modify all rules on Web Gateway to let them perform the actions that you consider appropriate.

• **Fields of web security** — A web security policy usually covers different fields of web security. Such fields are, for example
  
  • Protection against viruses and other malware
  • Control of access to web objects with particular URLs
  • Media type filtering to exclude downloads consuming overmuch bandwidth.

  Different fields of web security are usually covered by different rule sets on Web Gateway.

  Some fields are already covered by default rule sets after the initial setup. You can extend the coverage for these fields and also include additional fields by importing rule sets from a built-in or an online library.

• **Cloud use** — The rules of your web security policy are applied to the traffic that is created by the web usage of the users of your organization.

  Unless you configure it differently, however, the rules are only applied to the web usage of those users who access the web from inside your local network. This kind of usage is also known as on-premise use.

  You can, however, enable one or more rule sets for cloud use. This means that the rules in these rule sets are also enforced when users of our organization access the web from outside your local network.

• **Filtering process** — The activities that are performed by rules on Web Gateway can be seen as parts of a comprehensive filtering process. This process filters web traffic that is caused by the web usage of the users within your network.

  The process blocks attempts to access the web that do not comply with your web security policy and allows those that are compliant.
The process is performed in different cycles.

- A request cycle for filtering requests for web access performed by users
- A response cycle for filtering responses to requests sent by web servers
- An embedded objects cycle for filtering objects, such as files and archives, that are sent embedded in requests or responses.

Only one filtering cycle is going on at a particular point in time on Web Gateway.

The rule sets of your web security policy can be differently configured with regard to these cycles. A particular rule set can apply to all cycles, or only to one, or to any combination of them.

Contents
- Configuring a web security policy
- Fields of web security and rule sets
- Access a rule set
- Rule sets
- Filtering process
- Common tasks in policy configuration

Configuring a web security policy

A web security policy is implemented on Web Gateway, which includes various rules. When a situation arises where a rule applies, it performs an action. You can configure this policy by modifying its rules to adapt them to the needs of your organization.

To configure a web security policy, you modify its rules, dealing with them on different levels.

- Rule sets — Rules are grouped in rule sets, each of which usually covers a particular field of web security, for example, anti-malware filtering, URL filtering, media type filtering, and others.

A default system of rule sets is implemented on Web Gateway during the initial setup.

You can enable or disable these rule sets, move, copy, and delete them, modify their rules, import rule sets from a built-in or an online library, and create rule sets of your own.

The rules in these rule sets are applied to the traffic that is created by the web usage of the users of your organization. Unless you configure it differently, the rules are only applied to the web usage of users who access the web from inside your local network.

You can, however, enable one or more rule sets for cloud use. The rules in these rule sets are then enforced even when users of our organization access the web from outside your local network.

- Rules — You can enable and disable individual rules, move, copy and paste them, delete them, and create rules of your own.
• **Rule elements** — As default rules are already implemented on Web Gateway, you will usually configure individual elements of rules rather than creating completely new rules. The following are rule elements that you might deal with more often.

• **Properties** — Every rule contains at least one property. A property in a rule on Web Gateway is usually a property of a web object or an entity that is related to a web object, such as the user who requests access to it.

A property of a web object is, for example, Antimalware.Infected. If this property has the value true for a web object that access is requested to, a default rule on Web Gateway, which contains this property, blocks the request and, consequently, denies the user access.

• **Lists of web objects** — Lists of web objects are used within rules, for example, to make sure that access to these objects is not impeded by a particular blocking rule.

A rule that uses a list like this might stop processing for all rules that would otherwise be processed after it, including the blocking rule.

• **Module settings** — Property values are found by modules of the filtering process on Web Gateway. These modules are also known as filters or engines. You can configure settings for these modules to let them complete their jobs in different ways.

For example, to find out whether the value of the Antimalware.Infected property is true for a requested web object, the object must be scanned for infections. This process is handled by the Anti-Malware module.

By configuring settings for this module, you can, for example, involve the Gateway Anti-Malware engine in the scanning process combined with additional scanning by Advanced Threat Defense.

---

### Fields of web security and rule sets

Different fields of web security are usually covered by different rule sets on Web Gateway.

Some fields are already covered after the initial setup. You can cover more fields later on by importing rule sets from a built-in or an online library.

### Fields of web security covered by default rule sets

The fields of web security listed in the following are covered by default rule sets after the initial setup of Web Gateway.

These fields belong to the larger field of web filtering, which means they are related to threats and other issues that might arise when users of your local network access the web.

• **Anti-malware filtering** — Covered by the Gateway Anti-Malware rule set.

• **URL filtering** — Covered by the URL Filtering and Dynamic Content Classification rule sets.

  The Dynamic Content Classification rule set contains rules for performing URL filtering using additional categorization methods.

• **Media type filtering** — Covered by the Media Type Filtering rule set.

• **Global whitelisting** — Covered by the Global Whitelist rule set.
• **SSL scanning** — Covered by the SSL Scanner rule set.
  This rule set is available by default, but not enabled.

• **Functions in support of web filtering** — Covered by the Common Rules rule set.
  This rule set has several nested rule sets, which deal with web caching, archive opening, indication of download progress, and other fields of support for web filtering.

### Fields of web security covered by library rule sets

Many fields of web security that are not covered by default rule sets on Web Gateway, can be covered by importing rule sets from the built-in and the online rule set libraries.

#### Built-in rule set library

The following are fields of web security that are covered by rule sets from the built-in library. Some fields of web security that are basically covered by default rule sets can obtain additional coverage by library rule sets.

• **Anti-malware filtering** — Covered by the rule sets in the Gateway Anti-Malware section of the built-in library.

• **Application filtering** — Covered by the rule sets in the Application Control section of the built-in library.

• **Authentication** — Covered by the Authentication Server rule set and other rule sets in the Authentication of the built-in library.

• **Quota management** — Covered by the rule sets in the Quota/Coaching section of the built-in library.

#### Online rule set library

More policy fields can be covered by rule sets that you import from the online rule set library for Web Gateway.

Information about use and functions of each rule set is also provided in this library.

## Access a rule set

Access a rule set on the user interface of Web Gateway to work with its rules and their elements.

**Task**

1. Select **Policy | Rule Sets**.
   
   The **Rule Sets** tab appears showing the rule sets that are implemented in the navigation pane.

2. Click the rule set that you want to access.
   
   A view of the rule set appears in the configuration pane.

You can now work with the rules and rule elements of the rule set.

## 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 within a rule set system.

When a request for web access is received on the appliance, all rule sets in the system are processed for this request from top to bottom.

If 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 sent with requests and responses.
Working with the rule set system

During the initial setup of the appliance, a default system of rule sets is implemented. You can do the following to fine-tune this system and adapt it to the requirements of your network:

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

Default rule set system

The default rule system looks like this (nested rule sets are not shown).

Table 6-1 Default rule set system

<table>
<thead>
<tr>
<th>Rule set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass Microsoft (Office 365) Services (not enabled by default)</td>
<td>Lets requests and responses that are sent to and received from Office 365 and other Microsoft services bypass filtering.</td>
</tr>
<tr>
<td>SSL Scanner (not enabled by default)</td>
<td>Prepares SSL-secured web traffic for processing by other filtering functions.</td>
</tr>
<tr>
<td>Global Whitelist</td>
<td>Lets requests for whitelisted URLs or IP addresses skip further filtering.</td>
</tr>
<tr>
<td>Remove Privacy Violation Header</td>
<td>Removes privacy violation headers from requests to prepare them for processing by other filtering functions.</td>
</tr>
<tr>
<td>Common Rules</td>
<td>Provides functions that support the filtering process, such as web caching, progress indication, and opening of archives.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Controls filtering of individual URLs and URL categories.</td>
</tr>
<tr>
<td>Media Type Filtering</td>
<td>Controls filtering of particular types of media.</td>
</tr>
<tr>
<td>Gateway AntiMalware</td>
<td>Controls virus and malware filtering using virus signatures and proactive methods.</td>
</tr>
<tr>
<td>Dynamic Content Classification</td>
<td>Controls dynamic classification of content.</td>
</tr>
</tbody>
</table>

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 add a function that is missing in your system or when the implemented rule sets do not suit your network.

- The rule set library also contains 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.

In the standard rule set library, rule sets are grouped in categories, for example, authentication or URL filtering.

The following table shows the categories of the standard rule set library.
Table 6-2 Categories of library rule sets

<table>
<thead>
<tr>
<th>Rule set category</th>
<th>Includes rule sets for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Control</td>
<td>Filtering applications and individual functions of applications</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authenticating users</td>
</tr>
<tr>
<td>Coaching/Quota</td>
<td>Imposing quotas and other restrictions on the web access of users</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>Implementing single sign-on access to cloud applications</td>
</tr>
<tr>
<td>Common Rules</td>
<td>Supporting the filtering process, for example, by web caching, progress indication, or opening of archives</td>
</tr>
<tr>
<td>DLP</td>
<td>Implementing data loss prevention</td>
</tr>
<tr>
<td>ePO</td>
<td>Enabling use of the ePolicy Orchestrator</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Implementing error handling measures</td>
</tr>
<tr>
<td>Gateway Anti-Malware</td>
<td>Filtering web objects for infections by viruses and other malware</td>
</tr>
<tr>
<td>HTML/Script Filter</td>
<td>Filtering HTML pages and scripts</td>
</tr>
<tr>
<td>ICAP Client</td>
<td>Running an ICAP client on an appliance</td>
</tr>
<tr>
<td>Logging</td>
<td>Logging filtering and other activities</td>
</tr>
<tr>
<td>Media Type Filter</td>
<td>Filtering particular types of media</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Filtering mobile traffic</td>
</tr>
<tr>
<td>Next Hop Proxy</td>
<td>Using next-hop proxies for data transfer</td>
</tr>
<tr>
<td>Privacy</td>
<td>Modifying requests to ensure privacy</td>
</tr>
<tr>
<td>SiteAdvisor Enterprise</td>
<td>Using the SiteAdvisor for filtering request</td>
</tr>
<tr>
<td>SSL Scanner</td>
<td>Handling SSL-secured web traffic</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Performing troubleshooting measures</td>
</tr>
<tr>
<td>URL Filter</td>
<td>Filtering individual URLs and URL categories</td>
</tr>
<tr>
<td>Web Hybrid</td>
<td>Enabling synchronization with McAfee Web Gateway Cloud Service</td>
</tr>
</tbody>
</table>

Rule set views

The user interface provides two kinds of views for a particular rule set, the key elements view and the complete rules view.
Key elements view

The key elements view shows key elements of the rules in a rule set and allows you to configure them.

### Options of the key elements view

The following table describes the options of the key elements view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule set name field</td>
<td>Shows the default name of the rule set that key elements are displayed for and lets you edit this name.</td>
</tr>
<tr>
<td>Rule set description field</td>
<td>Shows the default description of the rule set that key elements are displayed for and lets you edit this description.</td>
</tr>
<tr>
<td>Enable</td>
<td>When selected, the rule set with the key elements that you are currently configuring is enabled.</td>
</tr>
<tr>
<td>Enable in Cloud</td>
<td>When selected, the rule set with the key elements that you are currently configuring is enabled for cloud use.</td>
</tr>
</tbody>
</table>
**Table 6-3 Options of the key elements view (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlock View</strong></td>
<td>Leaves the key elements view and displays the corresponding complete rules view.</td>
</tr>
<tr>
<td></td>
<td>- A confirmation message appears. Be aware that after leaving the key elements view, you cannot return to it unless you discard all changes or re-import the rule set.</td>
</tr>
<tr>
<td></td>
<td>On the rule sets tree, icons before the rule set name show which of the two views is currently enabled.</td>
</tr>
<tr>
<td></td>
<td>- Rule set in key elements view</td>
</tr>
<tr>
<td></td>
<td>- Rule set in complete rules view</td>
</tr>
<tr>
<td></td>
<td>- To work with nested rule sets, click <strong>Unlock View</strong> for the nesting rule set.</td>
</tr>
<tr>
<td></td>
<td>The nested rule sets appear on the rule sets tree, with the complete rule sets view enabled for each of them.</td>
</tr>
<tr>
<td></td>
<td>- To display the nested rule sets of the default <strong>Common Rules</strong> rule set, expand this rule set.</td>
</tr>
<tr>
<td></td>
<td>The complete rules view is already enabled for the last of the nested rule sets, while the others are still displayed in the key elements view.</td>
</tr>
<tr>
<td></td>
<td>You can use the <strong>Unlock</strong> option of the rule set context menu to leave the key elements view for one or more rule sets at once.</td>
</tr>
<tr>
<td></td>
<td>1 Select one rule set or several rule sets at once, then right-click and select <strong>Unlock</strong>.</td>
</tr>
<tr>
<td></td>
<td>2 Confirm that you want to leave the key elements view.</td>
</tr>
<tr>
<td></td>
<td>The complete rules view is enabled for all selected rule sets.</td>
</tr>
<tr>
<td></td>
<td>You can also expand a rule set that includes nested rule sets and select one or more nested rule sets.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Opens a window for configuring who is allowed to access the rule set with the key elements you are currently configuring.</td>
</tr>
<tr>
<td>Key elements for a rule set</td>
<td>The key elements vary for each rule set. Each group is preceded by a group header.</td>
</tr>
<tr>
<td></td>
<td>For example, on the key elements view for URL filtering, key elements are displayed in the groups <strong>Basic Filtering</strong>, <strong>SafeSearch</strong>, and others.</td>
</tr>
<tr>
<td></td>
<td>These groups contain key elements for basic URL filtering, for additionally using SafeSearch functions in the filtering process, and for other functions.</td>
</tr>
</tbody>
</table>

**Configure a key element**

The following is a sample task for configuring a key element of a web security rule.

A URL is entered into a URL whitelist. This whitelist is a key element of a rule in the default URL Filtering rule set.

When a request for access to a web object is received on Web Gateway, the rule lets the request skip URL filtering if the URL that is submitted with the request is on the whitelist. This reduces filtering effort and time for requests to access "allowed" web objects.

The URL entry in the sample is `http://www.mcafee.com/*`. Due to the wildcard element (`*`), all requests with URLs that match this entry, for example, `http://www.mcafee.com/us/products/web-gateway.aspx`, will skip URL filtering.
Task
1 Select Policy | Rule Sets.

2 On the rule sets tree, select the URL Filtering rule set. Key elements of the rules in this rule set appear in the configuration pane.

3 Under Basic Filtering, click Edit next to URL Whitelist. The Edit List window opens.

4 Enter a URL into the whitelist.
   a Under List content, click the Add icon. The Add Wildcard Expression window opens.
   b In the Wildcard Expression field, type http://www.mcafee.com/*.
   c Click OK.

5 Click OK. The Add Wildcard Expression window closes, and the URL appears in the list of the Edit List window.

6 Click Save Changes.

Complete rules view
The complete rules view shows the complete rules that are contained in a rule set. It allows you to work with their elements, including the key elements.

You can edit and delete rules and create rules of your own. You can also edit, delete, and create rule sets. New rule sets can be filled with existing rules, as well as with rules of your own.
You can also import rule sets from a rule set library on Web Gateway and from an online rule set library. You can work with these rule sets and their rules in the same way as with any other rules and rule sets.

Figure 6-2 Complete rules view

Configure a rule element in the complete rules view

The following is a sample task for configuring an element of a web security rule in the complete rules view.

A URL is entered into a URL whitelist. This whitelist is an element of a rule in the default URL Filtering rule set. The steps for accomplishing this are almost the same as for completing this task in the key elements view. Only the way the URL whitelist is accessed is different.

When a request for access to a web object is received on Web Gateway, a rule lets the request skip URL filtering if the URL that is submitted with the request is on the whitelist. This reduces filtering effort and time for requests to access "allowed" web objects.

The URL entry in the sample is http://www.mcafee.com/*.

Task

2. On the rule sets tree, select the URL Filtering rule set.
3. Click Unlock View to leave the key elements view.
4. Click Yes.

The complete rules view appears.
5 In the rule **Allow URLs that match in URL WhiteList**, click **URL WhiteList**.  
   The **Edit List** window opens.

6 Enter a URL into the whitelist.
   a Under **List content**, click the **Add** icon.
      The **Add Wildcard Expression** window opens.
   b In the **Wildcard Expression** field, type, for example, `http://www.mcafee.com/*`.
   c Click **OK**.
      The **Add Wildcard Expression** window closes, and the URL appears in the list of the **Edit List** window.

7 Click **OK**.
   The **Edit List** window closes.

8 Click **Save Changes**.
   For more information about working with rules and rule sets, see the **Rules** chapter.

---

**Filtering process**

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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All rules have been processed for each of the configured cycles and no rule has been found to apply.</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>A rule applies and requires that processing must stop completely.</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>A rule applies and requires that processing must stop for the current rule set.</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

Common tasks in policy configuration

The following are among the most common tasks when you are configuring a web security policy.

- **Configuring a rule element** — As default rules are already implemented in rule sets on Web Gateway, you will usually configure individual elements of rules rather than creating completely new rules. For example, you might want to fill or update a whitelist that is an element of a URL filtering rule.

- **Enabling a rule set for cloud use** — You can enable a rule set for cloud use. This means that you also want to enforce the rules of this rule set when users in your organization access the web from outside your local network.

Configuring a rule element

A rule on Web Gateway is composed of several elements. You can configure most of these elements to let the rule contribute in a particular way to your web security policy.

For example, a rule for URL filtering might use a whitelist to exempt URLs from filtering. Including a rule like this in a web security policy reduces filtering effort and time when requests to access web objects are considered no risk.

Several whitelisting rules are implemented by default on Web Gateway. Adding entries to a whitelist is therefore a common administrator activity.

Accessing a rule element

To access a rule element, you select the rule set that the rule with this element belongs to. For example, to access a whitelist in a rule for URL filtering, you select the rule set for URL filtering.
The name of the default rule set for URL filtering on Web Gateway is **URL Filtering**. If you select this rule set, several elements of its rules are displayed, for example, **URL Whitelist**. This element looks as follows:

![URL Whitelist](image)

**Figure 6-3 Sample rule element - URL Whitelist**

**Entering a value**

Clicking the **Edit** button next to the element field opens the whitelist for editing. You can, for example, enter the following:

http://www.mcafee.com/*

A request for web access with a URL that matches this entry is exempted from URL filtering. Due to the use of the wildcard symbol (*), there can be many matching requests, for example:


**Rule set views**

After selecting a rule set, you can access many rule elements without being shown the rules that these elements belong to. Alternatively, you can view the rules that particular rule elements belong to and access these elements from within their rules.

To enable access in either way, the user interface provides two views for most rule sets:

- **Key elements view** — This view shows the key elements of the rules in a rule set. Key elements are the elements that you will most likely want to work with when configuring the particular field of web security that is covered by the rule set.

  Working with this view saves you time when you are only interested in configuring a particular rule element and want to leave the remainder of the rule untouched.

  In some cases, a complete rule is treated as one element in the key elements view. This means that you can enable or disable the rule when working with this view.

  The key elements view is not available for:

  - A few default and library rule sets
  - Rule sets that you have created on your own

- **Complete rules view** — This view shows all the rules in a rule set. It shows them completely, which allows you to work with all elements that are available for the particular field of web security that is covered by the rule set.

  When working with this view, you can also delete rules or create rules of your own.

When you select a rule set, the key elements view is shown first. Before proceeding to the complete rules view, however, consider the following:

- You can proceed to the complete rules view of a rule set to review it and return to the key elements view, as long as you have not made and saved any changes in the complete rules view.

- After saving changes in the complete rules view, you cannot return to the key elements view unless you re-implement the rule set by importing it from the rule set library. The rule set is then provided in its initial state, which means that any changes that you made to the rule set before re-implementing it are lost.
Configuring a rule element in the complete rules view

In the complete rules view, you can view and configure a rule element from within the rule that it belongs to.

For example, the **URL Whitelist** element belongs to a default rule that can be paraphrased in plain text as follows:

*If the URL that a user submits in a request for web access matches one of the entries in the URL whitelist, skip filtering for this request and forward it immediately to the requested destination.*

On the user interface, this rule is shown in the following format:

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Name/Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allow URLs That Match in URL Whitelist</td>
<td></td>
<td>Stop Rule Set</td>
</tr>
<tr>
<td></td>
<td>URL matches in list URL Whitelist</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 6-4 Sample element within a complete rule - URL whitelist**

Clicking any instance of the **URL Whitelist** element in this rule opens the whitelist for editing. You can enter a value in the same way as when working with the key elements view.

Enabling a rule set for cloud use

Users in your organization who access the web from outside your local network are referred to as cloud users. To let a rule set that is implemented on Web Gateway apply to the web usage of these users, you must enable this rule set for cloud use.

The web usage of your cloud users is protected by McAfee WGCS, which is the partner product of Web Gateway within the integrated solution that is known as Web Protection. Enabling a rule set for cloud use on Web Gateway means that McAfee WGCS will apply these rules to protect the web usage of cloud users.

This way you can ensure that a common web security policy, or at least a policy that is the same for important fields of web security such as anti-malware or URL filtering, is enforced within your organization.

- Rule sets must be enabled for cloud use, as no rule set is cloud-enabled by default on Web Gateway.
- A warning informs you if you try to enable a rule set for cloud use that is not compatible with this use. In some cases, you can edit the rule set to make it compatible.
Complete rules

Working with complete rules allows you to configure all their elements. You can also delete rules and create new rules of your own.

Contents
- Rule elements
- Rule format on the user interface
- Rule representation in the documentation text
- Create a rule
- Create a rule set
- Import a rule set
- Restrict access to a rule set

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.

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.

![Rule format on the user interface](image)

Figure 7-1 Format of a rule on the user interface
The following table explains the meaning of the rule elements.

Table 7-1 Elements of a rule on the user interface

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Allows you to enable or disable the rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the rule</td>
</tr>
<tr>
<td>• Block URLs ... — Name text</td>
<td></td>
</tr>
<tr>
<td>• Category <strong>BlockList</strong> (in rule name) — List used by the rule</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clicking on the list name opens the list for editing.</td>
</tr>
<tr>
<td>• Yellow triangle (next to a list name) — Indicates that the list is initially empty and you need to fill the entries.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 7-1  Elements of a rule on the user interface (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong></td>
<td>Criteria of the rule</td>
</tr>
<tr>
<td></td>
<td>The criteria is only visible after clicking the Show details toggle button.</td>
</tr>
<tr>
<td></td>
<td>• URL.Categories — Property</td>
</tr>
<tr>
<td></td>
<td>• &lt;Default&gt; — Settings of the module that retrieves a value for the property</td>
</tr>
<tr>
<td></td>
<td>For example, the Default settings that appear here are settings of the URL Filter module.</td>
</tr>
<tr>
<td></td>
<td>• URL.Categories — Property</td>
</tr>
<tr>
<td></td>
<td>• &lt;Default&gt; — Settings of the module that retrieves a value for the property</td>
</tr>
<tr>
<td></td>
<td>For example, the Default settings that appear here are settings of the URL Filter module.</td>
</tr>
<tr>
<td></td>
<td>• at least one in list — Operator</td>
</tr>
<tr>
<td></td>
<td>• Category BlockList — Operand (also known as parameter)</td>
</tr>
<tr>
<td></td>
<td>• Yellow triangle (next to a list name) — Indicates that the list is initially empty.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Action of the rule</td>
</tr>
<tr>
<td></td>
<td>• Block — Name of the action</td>
</tr>
<tr>
<td></td>
<td>• &lt;URLBlocked&gt; — Settings of the action</td>
</tr>
<tr>
<td></td>
<td>• Statistics.Counter. Increment — Name of the event</td>
</tr>
<tr>
<td></td>
<td>• “BlockedByURLFilter, 1” — Parameters of the event</td>
</tr>
<tr>
<td></td>
<td>• &lt;Default&gt; — Settings of the event</td>
</tr>
<tr>
<td></td>
<td>• Statistics.Counter. Increment — Name of the event</td>
</tr>
<tr>
<td></td>
<td>• “BlockedByURLFilter, 1” — Parameters of the event</td>
</tr>
<tr>
<td></td>
<td>• &lt;Default&gt; — Settings of the event</td>
</tr>
</tbody>
</table>

### Rule representation in the documentation text

When rules are explained in the Web Gateway documentation, different ways of representing them within the documentation text are used.

A rule can be represented in a long or short format, providing more or less explicit information about the structure of a rule. The individual elements of a rule can be marked using different fonts to distinguish them from each other or all appear in the same font.
The long and the short formats can both be combined with different element markup to represent rules as follows:

- **Short rule representation** — A rule is represented in a short format with different fonts used for the individual rule elements.
- **Short unified rule representation** — A rule is represented in a short format with the same fonts used for all rule elements.
- **Long rule representation** — A rule is represented in a long format with different fonts used for the individual rule elements.
- **Long unified rule representation** — A rule is represented in a long format with the same fonts used for all rule elements.

All rule representations are followed by explanations of the respective rules in plain text.

**Rule representation on the user interface**

On the user interface of Web Gateway, a rule looks like this. The three main rule elements (criteria, action, and events) are each shown in a separate column. The rule name appears in bold above the rule criteria.

![Figure 7-2 Rule representation on the user interface](image)

In this sample representation, the rule name and elements are as follows:

- **Name** — Block if virus was found
- **Criteria** — Antimalware.Infected<Gateway Anti-Malware> equals true
- **Action** — Block<Virus Found>
- **Event** — Statistics.Counter.Increment("BlockedByAntiMalware",1)<Default>

The different representation methods used in the documentation text all rely in one way or other on how a rule is represented here.

**Short rule representation**

The short rule representation shows the main elements of a rule next to each other with the rule name in bold above the criteria. This representation method comes closest to the way that a rule is shown on the user interface.

To distinguish the main rule elements even further than it is done on the user interface, the criteria is shown in italics and the action is preceded by an arrow. The arrow symbolizes the relation between the criteria and the action (if the criteria matches, then the action is performed).

The rule event is always optional. It is also executed if the criteria matches, so it is just added after the action, separated by a dash.

**Block if virus was found**

Antimalware.Infected<Gateway Anti-Malware> equals true –> Block<Virus Found> – Statistics.Counter.Increment("BlockedByAntiMalware",1)<Default>
Short unified rule representation

The short unified rule representation differs from the short rule representation in that it does not use different fonts to distinguish the name from the rule elements and the rule elements from each other. It rather shows them all in narrow bold font.

Block if virus was found

Antimalware.Infected<Gateway Anti-Malware> equals true – Block<Virus Found> – Statistics.Counter.Increment ("BlockedByAntiMalware",1)<Default>

Long rule representation

The long rule representation shows each rule element in a separate row within a table, preceded by the element name. The rule name appears in red above the table like a section title.

Block if virus was found

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Antimalware.Infected&lt;Gateway Anti-Malware&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;Virus Found&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Statistics.Counter.Increment (&quot;BlockedByAntiMalware&quot;,1)&lt;Default&gt;</td>
</tr>
</tbody>
</table>

Long unified rule representation

The long unified rule representation differs from the long rule representation in that all individual rule elements are marked in narrow bold font.

Block if virus was found

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Antimalware.Infected&lt;Gateway Anti-Malware&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;Virus Found&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>Statistics.Counter.Increment (&quot;BlockedByAntiMalware&quot;,1)&lt;Default&gt;</td>
</tr>
</tbody>
</table>

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 132
  Configure name and enabling as general settings for a rule.
- Add the rule criteria on page 132
  Add the rule criteria to determine when a rule is applied.
- Add the rule action on page 133
  Add the action that is executed if the rule criteria matches.
- Add a rule event on page 134
  Optionally add one or more events that are executed if the rule criteria matches.
Name and enable a rule
Configure name and enabling as general settings for a rule.

Task
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.

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.
   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.

**Best practice:** If your criteria is to use a list as an operand, 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).
  
  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 list 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.

## 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 list.

   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 list 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 list, 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 a rule set

To restrict access to a rule set, complete the following procedure.

**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**
Lists

Lists are used by rules for 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
- Access a list
- Create a list
- Work with different types of lists
- External lists
- Subscribed lists
- Map Type lists
- Common Catalog
- JavaScript Object Notation data
List types

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

The following are the main list types:

- **Custom lists** — You can modify these lists. They are displayed on the upper branch of the lists tree on the Lists tab, for example, the list of URLs that are exempted from filtering.

  Custom lists can have entries in string, number, category, and other formats. Lists with different formats can require different methods of maintaining them. Some custom lists are initially empty and must have their entries filled by you.

  To the custom lists that Web Gateway provides after the initial setup, you can add lists that you create on your own.

- **System lists** — You cannot modify these lists. They are displayed on the lower branch of the lists tree on the Lists tab.

  System lists include category, media type, and application name lists, as well as lists of connectors used for cloud single sign-on. They are updated when an upgrade to a new version of Web Gateway is performed.

  System lists for Data Loss Prevention (DLP), application filtering, and the Dynamic Content Classifier can be included in automatic updates that you schedule.

- **Inline lists** — You can modify these lists, but they do not appear on the Lists tab. They appear inline as part of the settings for a configuration item, for example, a list of HTTP ports as part of the proxy settings.

- **Subscribed lists** — You set up these lists with a name on Web Gateway. They are initially empty and have their content retrieved from a data source that you subscribe to. Subscribed lists are displayed on the lists tree at the end of the custom lists.

  There are two subtypes of subscribed lists:

  - **McAfee-supplied lists** — Content for these lists is retrieved from a McAfee server.

    A number of lists are available on the McAfee server, for example, lists of IP address ranges or media types.

  - **Customer-maintained lists** — Content for these lists is retrieved from a data source that you specify.

    Sources that you can specify are files on web servers running under HTTP, HTTPS, or FTP.

List content is retrieved from the respective servers. To ensure that newer versions of this content are transferred to your lists on Web Gateway, you can perform updates manually or configure automatic updates.

- **External lists** — These lists reside on external sources under their own names. They have their content transferred to Web Gateway, where they provide the value of a property in a rule.

  External list content is transferred during runtime, which means it is retrieved when the rule with the external list property is processed.

  When the content has been retrieved, it is cached and reused until its date of expiration, which you can configure. After expiration, the transfer is repeated when the rule is processed again.

  Sources that content can be retrieved from include files on web servers running under HTTP, HTTPS, FTP, or LDAP, and in particular types of databases. They also include files that are stored within your local file system.
• **Map type lists** — These lists store pairs of keys and values that are mapped to each other. You can create map type lists and fill list entries on Web Gateway, or retrieve them as subscribed or external lists from other sources.

Keys and values on map type lists are initially stored in string format, but can be converted into different formats using suitable properties in rules.

• **Common Catalog lists** — These lists can be pushed from a McAfee ePO server to Web Gateway.

Common Catalog lists can have entries in IP address, domain name, string, or wildcard expression format. They are maintained on the McAfee ePO server.

### 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 141
  
  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 141
  
  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 142
  You can add a new list that you fill with entries later.
- Fill a list with entries on page 142
  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.

---

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 143
  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 144
  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 144
  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.

   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 is to 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 can 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.

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.

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 supplying subscribed lists or another server that you specify.

Subscribed lists that retrieve their content from the McAfee server are known as McAfee-supplied 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-supplied 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 managed remotely.

5. Configure settings for the list content.
   • For list content that is retrieved from the McAfee server:
     • Under Source, select McAfee-supplied 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.

### 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-supplied lists are updated together.

The content of McAfee-supplied 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.

#### Update subscribed lists supplied by the McAfee server

For subscribed lists that are supplied by the McAfee server, you must perform updates manually.

The content of McAfee-supplied 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-supplied lists is updated.

### Creating a content file for a customer-maintained list

When a subscribed list has been configured as a customer-maintained list, a content file describing the list structure must be created and stored on the web server that the content for this list is retrieved from.

A content file is created in txt or xml format, depending on whether it describes the structure of a simple or complex customer-maintained list. For simple lists, the content file can be created in both formats, for complex lists in xml format only.

Simple customer-maintained lists can be lists of the following types: Application Name, Category, Dimension, IP, IPRange, MediaType, Number, String, Wildcard Expression.

Complex customer-maintained can be lists of the following types: Certificate Authority, Extended List Element, HostAndCertificate, ICAP Server, NextHopProxy.
Content file for a simple list in txt format

The following is an example of a content file in txt format for a customer-maintained list of the Wildcard Expression type.

```
type=regex
"*.txt" "txt file extension"
"*.xml" "xml file extension"
```

The example illustrates the following conventions for a content file in txt format.

- The first line in the file specifies the type of the customer-maintained list that the content file is provided for. The format is: `type=<list type>`

  For the list type, one of the following terms must be used: `applcontrol, category, dimension, ip, iprange, mediatype, number, string, regex`.

- The lines below the first line are for list entries in the customer-maintained list.

  A line contains as many items as a list entry in the customer-maintained list. Each item is included in double quotes.

  An entry in a list of the Wildcard Expression type contains two items. One is the wildcard expression, the other is a comment that describes the wildcard expression.

The following example illustrates some more conventions for a content file.

```
type=string
"withoutDescription"
"emptyDescription" ""
"data with description and more spaces in-between" "description"
"data with spaces*    " "description"
"Hello\"Michael\" "Michael!\"" ""
```

- An entry in a list of the String type also contains two items: the string and a comment that describes it. However, the description can be omitted.

  If the description is omitted, the item for it in the content file can also be omitted, which is shown in line 2.

- Alternatively, if the description is omitted, this can be represented by two double quotes with nothing in between, as shown in line 3.

  The line also illustrates the following:

  - Double quotes occurring in a string must be masked by a following backslash.
  - A backslash that does not follow on double quotes represents itself (a backslash).
  - Non-alphanumerical characters, such as the * (asterisk), are allowed at the beginning of a string.

On the user interface, the list entry specified in line 3 would look as follows: `*emptyDescription\""`

- If multiples spaces are inserted between items in the content file, they are ignored in the list entries of the customer-maintained file.

  On the user interface, the entry specified in line 4 would therefore look as follows: `"data with description and more spaces in-between" "description"`
• Multiple spaces within a string in a content file are also ignored in the list entry of the customer-maintained list.

So, on the use interface, the entry specified in line 5 would look as follows: "data with spaces* " "description"

• Line 6 illustrates several of the already mentioned conventions.

Content file for a simple list in xml format

The following is an example of a content file in xml format for a customer-maintained list of the Wildcard Expression type. The list content is the same as in the first example of the preceding subsection.

```xml
<content type="regex">
    <listEntry>
        <entry>*.txt</entry>
        <description>txt file extension</description>
    </listEntry>
    <listEntry>
        <entry>*.xml</entry>
        <description>xml file extension</description>
    </listEntry>
</content>
```

For the content type, the same terms must be used as for a content file in txt format.

Content files for complex lists

Manually creating a content file for a complex customer-maintained list is rather difficult. However, you can use the options of the user interface to export an existing complex list and store it in a file.

In this file, the complex list appears in xml format. If you delete all lines in the file that precede the opening `<content>` tag and follow the closing `</content>` tag, you almost get a content file for that complex list.

Then you only need to modify the opening `<content>` tag to read `<content type="\<file type>\"`, for example, `<content type="nexthopproxy">`.

The terms you can use to specify the file type are: ca, extendedlist, icapserver, hostandcertificate, nexthopproxy.

Best practice: Working with a McAfee-supplied subscribed list

You can use a subscribed list that is supplied by McAfee in a rule of your web security policy, for example, to let particular traffic bypass SSL scanning.

Web traffic might be sent from the clients of your corporate network to particular destinations, for example, WebEx applications, using SSL-secured connections. When this traffic is received on Web Gateway, you might want to let it skip SSL scanning.

For this purpose, you need a list with the IP address ranges that are used by WebEx. As these addresses change frequently, McAfee supplies an address list, which is updated in intervals, saving you the effort of keeping this list up to date manually.

The list is included in the update schedule that you configure on Web Gateway to make sure that any updates supplied by McAfee are eventually passed on to your Web Gateway appliance or to all the appliances that you are running in a Central Management configuration.

To use this McAfee-supplied list in your web security policy:

• Create an empty list of your own and let this list be filled with WebEx address ranges from the McAfee list

• Set up a rule that uses your list to let requests for accessing WebEx destinations skip SSL scanning
Use a McAfee-supplied subscribed list in a rule

To use a McAfee-supplied subscribed list in a rule that performs a suitable action on web traffic to particular destinations, configure the list as part of the rule criteria.

**Task**

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

2. On the rule sets tree, select the **SSL Scanner** default rule set and click **Unlock View** to view the complete rules view.

3. Make sure the rule set is enabled and select the nested **Handle CONNECT Call** rule set.

4. Click **Add Rule** and in the window that opens configure a rule as follows.
   a. Under **Name**, type the rule name, for example, **Bypass SSL scanning for WebEx destinations**.
   b. Under **Criteria**, configure the following:
      • Property: **URL.Destination.IP**
      • Operator: **is in range list**
      • Compare with (operand): **WebEx IP Ranges**
   c. Under **Action**, select **Stop Rule Set**.
   d. Click **Finish**.
      The window closes and the rule appears at the end of the rules in the rule set.
   e. Move the rule into first position.

5. Click **Save Changes**.

Requests for destinations with the IP addresses on the WebEx list will now bypass SSL scanning on Web Gateway.

Create a McAfee-supplied subscribed list with IP address ranges

To create a subscribed list with IP address ranges for WebEx applications that is maintained by McAfee, create a list of your own and let its content be provided by a McAfee-supplied list.

**Task**

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

2. Above the lists tree, click the **Add** icon.

3. In the **Add List** window, configure a list as follows.
   a. Configure general settings for the list:
      • **Name**: **WebEx Subscribed List** or any other suitable name
      • **Type**: **IPRange**
   b. Select **List content is managed remotely**.
   c. Select **McAfee-supplied** and click **Choose**.
   d. In the **Choose List Content** window, select the list named **WebEx IP Ranges**.

Lists

Subscribed lists

McAfee Web Gateway 7.8.0

Product Guide 153
4 Click **OK** in both windows.

The list appears on the **Subscribed Lists** branch of the lists tree

5 Click **Save Changes**.

You can now use the list that you have created in a suitable rule.

---

**Map Type lists**

Map Type lists, also known as maps, can be used to store pairs of keys and values mapped to each other. Both the keys and their values are of the string type.

Lookup operations can be performed on existing maps, for example, to find out whether a particular key exists in a map or what value is mapped to a key.

Other operations include setting and deleting values for a particular key or converting a complete map into a single string.

You can create and fill Map Type lists on the user interface of Web Gateway or retrieve them from a remote location using the external lists and subscribed lists functions.

If you want to work with other data types for your maps, for example, numbers or IP addresses, you can convert them using properties such as `Number.ToString` or `IP.ToString`.

**Create a Map Type list**

To create a Map Type list, add a list of this type and fill it with pairs of keys and values.

**Task**

1 Select **Policy | Lists**.

2 Above the lists tree, click the **Add** icon.

   The **Add List** window opens.

3 Add a MapType list.
   a In the **Name** field, type a list name.
   b From the **Type** list, select **MapType**.
   c Click **OK**.

   The window closes and the new Map Type list appears on the lists tree under **Custom Lists | MapType**.

   The settings pane is ready for filling the list with entries.

4 Click the **Add** icon on the settings pane.

   The **Add Map Type** window opens.

5 For each pair of entries, you need to fill the list as follows.
   a In the **key** field, type a key name.
   b In the **value** field, type a value.
   c Click **OK**.
The window closes and the pair of entries appears in the first row on the settings pane.

6. Click **Save Changes**.

**Using properties to work with Map Type lists**

There are several properties for working with Map Type lists. Using these properties in rule criteria, you can retrieve information about a Map Type list, modify a list, create a new list, and also convert a list into a string.

To retrieve information about a Map Type list (map), you can:

- Retrieve a map that you specify a name for
- See whether a particular key exists within a map
- Retrieve the number of key-value pairs in a map
- Retrieve a list of the keys in a map
- Retrieve the value for a given key in a map

The following properties are used to perform these activities.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.ByName</td>
<td>Provides a map with the name that you specified.</td>
</tr>
<tr>
<td>Map.HasKey</td>
<td>Is true if the specified map includes the specified key.</td>
</tr>
<tr>
<td>Map.Size</td>
<td>Provides the number of key-value pairs in a map.</td>
</tr>
<tr>
<td>Map.GetKeys</td>
<td>Provides a list of the keys in a map.</td>
</tr>
<tr>
<td>Map.GetStringValue</td>
<td>Provides the string that is the value of the specified key in the specified map.</td>
</tr>
</tbody>
</table>

You can, for example, use the `Map.GetStringValue` property in the criteria of a rule to see whether a key in a list has a particular value. The key could be a user name and the value a string that serves as a token for authentication.

The criteria would then be configured as follows:

`Map.GetStringValue (testmap, "sampleuser") equals "sampletoken"`

If the `sampleuser` key has `sampletoken` as its value, the criteria matches, and the rule executes a particular action, for example, **Continue**.

When a map is modified, the modification is applied to a copy of the original map, while the original map itself remains unmodified. To modify a map in this way, you can:

- Set a key to a particular value
- Delete a key

The following properties are used to perform these activities.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.SetStringValue</td>
<td>Provides a map in which the specified value is set for the specified key.</td>
</tr>
<tr>
<td>Map.DeleteKey</td>
<td>Provides a map in which the specified key is deleted.</td>
</tr>
</tbody>
</table>

To create a new map or convert a map into a string, the following properties are used.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.CreateStringMap</td>
<td>Provides a new map, which is still empty.</td>
</tr>
<tr>
<td>Map.ToString</td>
<td>Provides a map converted into a string.</td>
</tr>
</tbody>
</table>
Retrieving map data from external and subscribed lists

Data for Map Type lists (maps) can be retrieved from external and subscribed lists.

External lists

For retrieving map data from an external list, the ExtLists.StringMap property is provided, which you can use in the criteria of a suitable rule. The value of this property is a list of maps that have an external list as their source.

For example, to find out whether a particular key is contained in a list that is retrieved from an external source, you can configure the following rule criteria:


To specify the external list and where it can be retrieved from, you need to configure the settings of the External Lists module, which is the module that performs the retrieval. In the above criteria, these settings appear under the name of External Lists.

External list data can be retrieved from a web service, a file, a PostgreSQL or SQLite3 database, or using LDAP. For these source types, the following must be observed when configuring the retrieval of data for a map:

- Web service or file

  The type of data that is retrieved from a web service or a file must be Plain Text.

  To locate the data, a regular expression is used that includes two parts. The first part is for the keys, the second for the values.

- Databases

  The database query for retrieving the data must return two columns. The first column delivers the keys, the second column delivers the values.

- LDAP

  To retrieve the data, a first and a second attribute are configured within the LDAP settings. The first attribute delivers the keys, the second attribute delivers the values.

Subscribed lists

Entries in subscribed lists that map data is retrieved from must have the following format.

```xml
<listEntry>
  <complexEntry defaultRights="2">
    <configurationProperties>
      <configurationProperty key="key" type="com.scur.type.string" value="key"/>
      <configurationProperty key="value" type="com.scur.type.string" value="value"/>
    </configurationProperties>
  </complexEntry>
  <description>
  </description>
</listEntry>
```

Within the listEntry element, there's a complexEntry embedded. This allows the Subscribed Lists module to process the format.
Common Catalog

The Common Catalog provides lists that can be pushed from a McAfee ePO server to a Web Gateway appliance. The following types of lists can be pushed: IP address, domain name, string, wildcard expression.

- **Do not modify the content of the lists on the Web Gateway appliance, because this content is updated in intervals on the McAfee ePO server. These updates will overwrite any changes that you might have applied.**

A REST (Representational State Transfer) interface runs internally on both systems to enable the list transfer. A McAfee ePO extension for Web Gateway must also be running on the McAfee ePO server.

This extension includes a help extension, which provides online Help for handling the extension. An extension package is provided on the user interface of Web Gateway under the `ePolicy Orchestrator` system settings.

To let requests from the McAfee ePO server bypass filtering by web security rules on Web Gateway, you need to import a suitable rule set from the library, place it at the topmost position of the rule sets tree, and enable it.

In addition to this, you need to set up a McAfee ePO user account, as there must be an instance on the appliance that is allowed to handle the list transfer. For setting up this account, the `ePolicy Orchestrator` system settings are used.

The user of the McAfee ePO account must also appear as an administrator with an account among the internal Web Gateway administrator accounts.

After lists from the Common Catalog have been pushed to Web Gateway, 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.

Prepare the use of Common Catalog lists

To prepare the use of Common Catalog lists that are pushed from a McAfee ePO server to a Web Gateway appliance, complete the following high-level steps.

**Task**

1. Set up an account for a McAfee ePO user on Web Gateway.
2. Set up an administrator account with the same user name and password on Web Gateway.
3. Enable use of the REST interface on Web Gateway.
4. Import the Bypass ePO Requests rule set from the library on the user interface of Web Gateway, move it to the topmost position of the rule sets tree, and enable it.
5. Download a McAfee ePO extension package for Web Gateway and install it on the McAfee ePO server.
6. On the user interface of the McAfee ePO server, register a new server for communication with Web Gateway, specifying an appliance that Web Gateway runs on.

   - On the dashboard of the user interface, you should see, after about 15 minutes, data on web traffic that is processed on Web Gateway.

7. Push lists from the McAfee ePO server to Web Gateway.

   You should see the lists that you have pushed to Web Gateway on the lists tree of its user interface.

For more information on how to install a McAfee ePO extension package and perform activities on the McAfee ePO server, refer to the McAfee ePO documentation.
Set up a user account for Common Catalog lists
To enable the use of Common Catalog lists, you must set up a McAfee ePO user account on Web Gateway to create an instance that is allowed to handle the list transfer.

Task
1. Select Configuration | ePolicy Orchestrator.
2. Under ePolicy Orchestrator Settings, configure a user account.
   a. In the ePO user account field, leave the preconfigured value, which is epo.
   b. Next to the Password field, click Change.
      The New Password window opens.
   c. Use the window options to set a new password.
3. Make sure Enable data collection for ePO is selected.
4. Click Save Changes.

The user of the McAfee ePO account that you have configured must also appear as an administrator in an administrator account on Web Gateway.

Set up an administrator account for Common Catalog lists
To enable the use of Common Catalog lists, you must set up an administrator account on Web Gateway with the same user name and password as for the McAfee ePO user account.

Task
1. Select Accounts | Administrator Accounts.
2. Under Internal Administrator Accounts, click Add.
   The Add Administrator window opens.
3. Set up an administrator account for using Common Catalog lists.
   a. In the User name field, type epo.
   b. In the Password and Password repeated fields, type the password you configured when setting up the user account for the ePO user.
   c. From the Role list, select the ePO Common Catalog Administrator role.
   d. Click Edit to review the current role settings.
      The Edit Role window opens. Enable the following settings if necessary:
      • Policy — Lists accessible
      • Policy — Lists creation
      • REST Interface accessible
   e. Click OK.
      The window closes and the new administrator account appears under Internal Administrator Accounts.

Together with the user account for the McAfee ePO user, this administrator account serves as the instance on Web Gateway that must exist for handling the transfer of lists from a McAfee ePO server.
Enable use of the REST interface for Common Catalog lists

For communication with the McAfee ePO server that Common Catalog lists can be transferred from, you need to enable the internal REST (Representational State Transfer) interface on Web Gateway.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance that you want to transfer Common Catalog lists to and click **User Interface**.
3. Under **UI Access**, select both Enable Rest Interface over HTTP and Enable Rest Interface over HTTPS.
4. Under **Login Page Options**, select Allow multiple logins per login name.
5. Click **Save Changes**.

Sample settings for registering Web Gateway on a McAfee ePO server

To transfer Common Catalog lists to a Web Gateway appliance, you must register the appliance as a new server on the McAfee ePO server.

The following are sample settings for this registration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server type</td>
<td>McAfee Web Gateway 7</td>
</tr>
<tr>
<td>Name</td>
<td>mwg7-3.sample-lab.local</td>
</tr>
<tr>
<td>Notes (optional)</td>
<td></td>
</tr>
<tr>
<td>Host name</td>
<td>mwg7-3.sample-lab.local</td>
</tr>
<tr>
<td>Host address</td>
<td>171.18.19.226</td>
</tr>
<tr>
<td>Administration port</td>
<td>4712</td>
</tr>
<tr>
<td>Statistics retrieval port</td>
<td>9090</td>
</tr>
<tr>
<td>User name (for access to the host GUI)</td>
<td>&lt;Initial or current user name for access to the Web Gateway user interface&gt;</td>
</tr>
<tr>
<td>Password</td>
<td>&lt;Initial or current password for access to the Web Gateway user interface&gt;</td>
</tr>
<tr>
<td>User name (for statistics retrieval and list management)</td>
<td>epo</td>
</tr>
<tr>
<td>Password</td>
<td>&lt;Same password as the one that was configured for the ePO user and administrator accounts on Web Gateway&gt;</td>
</tr>
<tr>
<td>Options</td>
<td>Allow ePO to manage lists on this system (enabled)</td>
</tr>
</tbody>
</table>

The initial user name and password for access to the user interface of Web Gateway are `admin` and `webgateway`.

JavaScript Object Notation data

Data that is encoded in JavaScript Object Notation (JSON) format can be read, modified, and created on Web Gateway.

JavaScript Object Notation is a text-based data-interchange format. It can be read easily by JavaScript, but is not tied to using this language. The notation is used for communication with interactive websites, as well as with NoSQL and document-oriented databases, for example, MongoDB or Couch DB.
JSON-based programming interfaces exist for use in well-known social networks, such as Facebook or Twitter.

On Web Gateway, JSON data is used, for example, in scanning reports that are provided by McAfee® Advanced Threat Defense (Advanced Threat Defense). Lists that are retrieved from external sources and processed on Web Gateway can also be in JSON data format.

**JSON data**

JSON data is made available in what is called objects. A JSON object is a container that includes data of the same or of different ordinary types, such as strings, numbers, and others.

The basic structure of a JSON object can be represented as follows:

```json
object: { "key": value,  "key": value, ...
```

For example:

```json
Employee: { "First name": "Joe",  "Last name": "Miller",  "Age": 32
```

The value of a JSON element can be data of the following types: string, number, Boolean, null.

A JSON object can also include an array:

```json
object: { "key": value,  "key": value,  array: [value, value, ...]
```

For example:

```json
Employee: { "First name": "Joe",  "Last name": "Miller",  "Children": [Ian, Lisa]
```

In original JavaScript Object Notation, only objects and arrays can occur at the top level of a hierarchical data structure. However, when it is supported on Web Gateway, a simple element can also occur in top-level position.

A JSON object can also be embedded in another JSON object.

**Using properties to handle JSON data**

Several properties are available on Web Gateway for reading, modifying, and creating JSON data.

For example, the `JSON.FromString` property is used to create a JSON element from a string. The string is specified as a parameter of the property. So `JSON.FromString("Miller")` delivers the string "Miller" as the value of a JSON element.

A JSON object is created using the `JSON.CreateObject` property. This object is initially empty. To store a JSON element inside an object, you need to identify both items by giving them names.

An object is given a name by making it a user-defined property, which is always configured with a name.

For example, you can create a user-defined property under the name `User-Defined.myjsonemployee` and then use an event in a rule to give it the value of the `JSON.CreateObject` property.

**Name**

**Create JSON object as user-defined property**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt;</td>
<td>Set User-Defined.myjsonemployee = JSON.CreateObject</td>
</tr>
</tbody>
</table>

The empty JSON object `User-Defined.myjsonemployee` can be filled using the `JSON.StoreByName` property, which has parameters for object name, element key, and element value.
For example, the following stores an element with the key "Last name" and the value "Miller" in the object:

```javascript
JSON.StoreByName(User-Defined.myjsonemployee, "Last name", JSON.FromString("Miller"))
```

Storing an element inside an object can also be performed in a simpler way:

- You need not create the object before using the JSON.StoreByName property.
  - Specifying the object name as a parameter of the property creates the object if it did not exist before.
- You need not use the JSON.FromString property to obtain the element value.
  - Specifying a string directly also creates this value. The same applies to the other ordinary data types that the value of a JSON element can have.

So, the following also stores an element inside an object:

```javascript
JSON.StoreByName(User-Defined.myjsonemployee, "Last name", "Miller")
```

**Groups of JSON properties**

Many JSON properties are similar to other properties in that they are used to perform the same kind of data handling activity.

The JSON.From<x> properties, for example, JSON.FromString, deliver a JSON element that has the value of a simple data type. The value of the simple data type is specified as the parameter of the JSON property.

The following are some important groups of JSON properties:

- **JSON.From<x>** = Delivers a JSON element that has the value of a simple data format
  
  Properties: JSON.FromString, JSON.FromNumber, JSON.FromBool, JSON.FromStringList, JSON.FromNumberList

- **JSON.As<x>** = Delivers the value of a JSON element in a simple data format
  
  The properties of this group are used to perform an operation that is the reverse of what the JSON.From<x> properties do.
  
  For these properties to work correctly, the format of the JSON element must match the simple data format.
  
  For example, the JSON.AsString property will only deliver a (simple) string if the value of the JSON element is a (JSON) string.
  
  Properties: JSON.AsString, JSON.AsNumber, JSON.AsBool

- **JSON.Create<x>** = Creates a JSON object, array, or the element value 0.
  
  Properties: JSON.CreateObject, JSON.CreateArray, JSON.CreateNull

- **JSON.Get<x>** = Delivers a JSON element from within an object or the data type of an element
  
  JSON.GetByName delivers an element that is identified by its key from within a JSON object.
  
  JSON.GetAt delivers an element that is identified by its position within a JSON array.
  
  JSON.GetType delivers the type of an element.

**Using JSON properties in filtering rules**

The JSON.ToString property delivers the value of a JSON element in string format.

You can use this property, for example, in a simple rule to whitelist a particular client IP address.
In this rule, a given client IP address is compared to the client IP address you want to whitelist to see whether both addresses match.

Name

**Allow client IP address provided as JSON element value**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client.IP equals String.ToIP(JSON.ToString(User-Defined.myjsonipaddress))</td>
<td>StopCycle</td>
</tr>
</tbody>
</table>

The client IP address that is to be whitelisted is provided as the value of the user-defined property **User-Defined.myjsonipaddress**.

The JSON.ToString property delivers this value in string format. The String.ToIP property converts the string back into an IP address, so it can be compared to the address that is the value of the Client.IP property at the beginning of the rule.

Before the UserDefined.myjsonipaddress property can be used in the sample rule, you must create it in JSON data format and set its value to the address that is to be whitelisted.

To set the value, you can use an event in another sample rule, as shown in the following.

Name

**Set value of JSON type user defined property to client IP address**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt; Continue</td>
<td>Set User-Defined.myjsonipaddress = JSON.FromString(&quot;10.149.8.34&quot;)</td>
</tr>
</tbody>
</table>

The JSON.FromString property in the rule event converts the client IP address, which is specified as a property parameter in string format, into the value of a JSON element.

**Retrieving JSON data from an Advanced Threat Defense report**

When Advanced Threat Defense is called by a rule on Web Gateway to scan a web object, the scanning result is stored as the value of the **Antimalware.MATD.Report** property.

The result is provided as a string that has the elements of the result arranged in JSON style. It can be converted into a JSON element, using the JSON.ReadString property. This property takes the AntiMalware.MATD.Report property as a parameter.

The JSON element can then be set as the value of a user-defined property.

The rule that uses these properties could look as follows:

Name

**Set value of JSON type user defined property to Advanced Threat Defense report**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt; Continue</td>
<td>Set User-Defined.myjsonmatdreport = JSON.ReadFromString(Antimalware.MATD.Report)</td>
</tr>
</tbody>
</table>

You can retrieve the data of the result using the JSON.GetByName property and, for example, write it into a log file.

Name

**Write JSON data from Advanced Threat Defense report into log file**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In the event of this rule, "Summary" is the key of a JSON element that has the data of a scanning result as its value. This key and its value are contained in a JSON object, which is the value of the Antimalware.MATD.Report property.

The structure of the JSON object is shown in the following.

It contains several embedded objects. The element keys are the ones that are actually used in a report, while the values are examples.

```json
Report: {
  "Summary": {
    "Selectors": [
      {
        "Engine": "GAM engine",
        "MalwareName": "EICAR test file",
        "Severity": "5"
      }
    ],
    "Verdict": {
      "Severity": "5",
      "Description": "Subject is malicious"
    },
    "Stats": [
      {
        "ID": "0",
        "Category": "Persistence, Installation Boot Survival",
        "Severity": "5"
      }
    ]
  }
}
```

**Retrieving external lists in JSON data format**

For handling JSON data in a list that has been retrieved from an external source, the `Ext.Lists.JSON` property is available. After retrieving the external list, the list content is a JSON element that is the value of this property.

Like all external list properties, `Ext.Lists.JSON` has three parameters in string format, which can be used to identify the external source.
Lists
JavaScript Object Notation data
Settings

Settings are used within Web Gateway for configuring modules (engines), rule actions, and system functions. Settings names 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.

After clicking a settings name, you can access and configure the parameters and values of the settings.

At the initial setup of the appliance, module and action settings are implemented together with the rule set system, as well as settings for the appliance system. Additional module and action settings are implemented when you import a rule set from the rule set library.

You can review and modify the initially implemented or imported settings. You can also completely delete module and action settings and create module and action settings of your own.

Contents
- Types of settings
- Access settings
- Create action and module settings

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 known 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.

---

**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 166**
  You can use the Settings tab to access settings for actions and modules.

- **Access action and module settings in a rule on page 167**
  You can click names of settings for actions and modules that appear in rules to access these settings.

- **Access system settings on page 167**
  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 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.
When the users of your network send requests for web access, Web Gateway 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 various ways. It is controlled by rules, which you can review and modify to adapt them to the requirements of your web security policy.

Default filtering on Web Gateway includes:

- **Anti-malware filtering** — Blocks access to web objects that are infected by viruses and other malware
- **URL filtering** — Blocks or allows access to web objects with particular URLs
- **Media type filtering** — Blocks or allows 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 of requests that are sent on SSL-secured connections.

### Contents
- **Anti-malware filtering**
- **URL filtering**
- **Media type filtering**
- **Application filtering**
- **Streaming media filtering**
- **Global whitelisting**
- **SSL scanning**
- **Hardware Security Module**
- **Advanced Threat Defense**
- **Data loss prevention**
- **Using an on-premise DLP server from the cloud**

### Anti-malware filtering

Anti-malware filtering ensures that the users of your network cannot access web objects that are infected by viruses and other malware. The filtering process detects infections and blocks access accordingly.

### Anti-malware filtering process

The anti-malware filtering process includes several elements, which contribute to it in different ways.

A default process for virus and malware filtering is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.
The process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- Whitelists are used in rules to let some web objects skip anti-malware filtering.
- The Anti-Malware module, which is called by a particular rule, scans web objects for infections by viruses and other malware.

**Rules for anti-malware filtering**

The rules that control anti-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.

When the default rule set system is implemented, a rule set for virus and malware filtering is included. Its name is Gateway Anti-Malware.

**Lists for anti-malware filtering**

The lists used in anti-malware filtering rules are mainly whitelists. Whitelists are used by whitelisting rules to let a 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. This module scans objects to detect infections by viruses and other malware.

According to the findings of this Anti-Malware, a blocking rule blocks access to web objects or lets them pass through.

When the 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 these submodules uses different scanning methods.

The two submodules are the Gateway Anti-Malware engine, and the Avira engine. The latter uses virus signatures to detect infections in web objects. This method can, however, only detect viruses and other malware that are already known and have been given signatures. To ensure a higher level of web security, the Gateway Anti-Malware engine also uses proactive methods to detect new viruses and malware.

When configuring settings for the Anti-Malware module, you can change the default mode, for example, to let the Avira engine run on its own,

To avoid temporary overloading of the submodules, you can configure an anti-malware queue that requests are moved to before being scanned.
Gateway Anti-Malware rule set

The Gateway Anti-Malware rule set is the default rule set for anti-malware filtering.

<table>
<thead>
<tr>
<th>Default rule set – Gateway Anti-Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**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.

Using this rule alone for whitelisting will cause a security problem because usually a client can set whatever user agent it prefers.

**Allow URL host that matches in list Anti-Malware URL Whitelist**

`URL.Host matches in list Anti-Malware 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.

**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.

**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 Web Gateway 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.

**Start Media Stream Scanner on streaming media and skip anti-malware scanning**

\[ \text{Cycle.Name equals "Response" AND StreamDetector.IsMediaStream<Default Streaming Detection> equals true} \rightarrow \text{Stop Rule Set – Enable Media Stream Scanner} \]

The rule uses the `Cycle.Name` property to check whether processing is in the response cycle and the `StreamDetector.IsMediaStream` property to check whether the web object that is sent in response to Web Gateway is streaming media.

If both are the case, processing of the rule set stops, so the remaining rule is not processed, and an event is used to start the Media Stream Scanner.

**Block if virus was found**

\[ \text{Antimalware.Infected<Gateway Anti-Malware> equals true} \rightarrow \text{Block<Virus Found> – Statistics.Counter.Increment(“BlockedByAntimalware”,1)<Default>} \]

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 Anti-Malware 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.

**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 Anti-Malware` 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 Anti-Malware*.  
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 Anti-Malware 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 Anti-Malware* (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.  

**Using URL information for anti-malware filtering**  
URL information is important for achieving accurate results in anti-malware filtering. Particular settings of the filter modules are required to make this information available.  

When the Gateway Anti-Malware engine scans files within anti-malware filtering on Web Gateway, it uses available information about the URL of a file to achieve a more reliable result. URL categories and reputation scores are an important part of this information.  

As URL filtering on Web Gateway is mainly handled by the URL Filter module (or engine), the Anti-Malware module (or engine), which is the module for anti-malware filtering, requests URL information from the URL Filter module. The URL Filter module retrieves this information from several sources, among them the Global Threat Intelligence system, depending on its settings.
To ensure that suitable information for the scanning process is passed on to the Gateway Anti-Malware engine, options that enable queries to the Global Threat Intelligence system must be configured for the Anti-Malware and URL Filter modules.

**Ensure the use of URL information for anti-malware filtering**

Ensure that information about URL categories and reputation scores from the Global Threat Intelligence system is made available to the scanning process in anti-malware filtering on Web Gateway.

**Task**

1. Select **Policy | Settings**.

2. Expand all settings that are configured for the **Anti-Malware** module (engine) and ensure that in the **Advanced Settings** section, the **Enable GTI file reputation queries** option is selected.

3. Select **Policy | Rule Sets** and ensure that the following applies.
   - There is a **Common Rules** rule set with a nested **Set URL Filter Internal Settings** rule set. These rule sets are part of the default rule set system. If they have been deleted or modified, import the default versions of these rule sets from the rule set library.
   - The nested **Set URL Filter Internal Settings** rule set contains the **Set URL Filter settings to be used by other filters** rule with the **URLFilter.SetInternalSettings** event.
     
     **The event settings, which are named Default, are the default settings of the URL Filter module.**

   - In the **Rating Settings** section of the event settings, **Use online GTI web reputation and categorization services if local ratings yields no result** is selected.

   **This option is selected and grayed out by default. It is still enabled as long as the Enable the Dynamic Content Classifier if local ratings yields no result option is selected, which is also true by default.**

   **If you deselect Enable the Dynamic Content Classifier if local ratings yields no result, Use online GTI web reputation and categorization services if local ratings yields no result remains selected, but is no longer grayed out.**

4. If you have modified any settings options or the rule set system, click **Save Changes**.

**Integrating TIE server information with anti-malware filtering**

You can integrate TIE server information with anti-malware filtering on Web Gateway, using this information in filtering rules and notifying the TIE server of critical scanning results found on Web Gateway.

A rule set is available in the library to implement this integrated filtering, providing several rules in addition to the rules in the **Gateway Anti-Malware** default rule set.

The additional rules integrate anti-malware filtering as performed by the filtering functions that are available on Web Gateway with information retrieved from a TIE server. The TIE server is in turn notified of critical filtering results found on Web Gateway.

**The integrated filtering is only applied to files with media type Executables.**

DXL messages are used to exchange information between Web Gateway and the TIE server. As parts of the DXL architecture are managed by a McAfee ePO server, Web Gateway must also be configured to connect to this administration device.
Property and event for exchanging information with a TIE server

The following property and event can be used in rules that handle information exchange with a TIE server.

- **TIE.Filereputation** — The value of this property is set to the reputation score that is queried and retrieved from a TIE server for a particular file.

  Processing of the property is performed by the TIE Filter module, which runs with particular settings.

- **TIE: Report file reputation** — This event sends a file reputation score to a TIE server. The score is based on the malware probability that the Gateway Anti-Malware (GAM) engine on Web Gateway finds after scanning a file.

  Scores are sent according to the scale of values used on a TIE server, corresponding to ranges of probability grades. For example, for a malware probability between 60 and 80, 30 is sent as a score to the TIE server.

Sample rule for using file reputation retrieved from a TIE server

The following sample rule uses TIE.Filereputation property to find out whether the reputation of a file that is processed on Web Gateway remains below a particular value. Information about the file reputation is retrieved from a TIE server.

If the file reputation actually remains below the configured value, an action is executed to block access to the file.

The blocking action runs with particular settings, which you can configure to provide a message to inform the user who requested the file about the blocking reason.

Name

Block after retrieving information about bad reputation from a TIE server

Criteria

| TIE.Filereputation less than or equals 30 |

Action

--> Block<TIE Reputation>

Sample rule for reporting file reputation to a TIE server

The following sample rule uses the TIE: Report file reputation event to send a file reputation score to a TIE server.

The score is based on the malware probability for a file that is processed on Web Gateway. The Antimalware.Infected and Antimalware.Proactive.Probability are used to find out about this probability.

If the probability exceeds the configured value, an action is executed to block access to the file. The TIE: Report file reputation event then sends a reputation score to a TIE server, which is based on the found probability range.

Name

Send information about file reputation to a TIE server

Criteria

| Antimalware.Infected<Gateway Anti-Malware with TIE> equals true AND Antimalware.Proactive.Probability<Gateway Anti-Malware> greater than or equals 90 |

Action

--> Block<Virus Found>

Event

TIE: Report File Reputation (1)
Configure integrating TIE server information with anti-malware filtering

To integrate TIE server information with anti-malware filtering, import the appropriate library rule set and configure settings for connecting to a McAfee ePO server.

Task
1. Implement the rule set for integrating TIE server information with anti-malware filtering.
   b. Import the Gateway Anti-Malware with TIE rule set from the library.
   c. On the rule sets tree, place the imported rule set immediately before the default Gateway Anti-Malware rule set and disable or delete the default rule set.

2. Configure settings for connecting to a McAfee ePO server.
   a. Select Configuration | Appliances.
   b. On the appliances tree, select the appliance that you want to connect to a McAfee ePO server and click ePolicy Orchestrator.
   c. Configure a host name, user account, and password for use by Web Gateway when connecting to a McAfee ePO server.
   d. Click Rejoining ePO for DXL communication to complete the setup.

   a. On the appliances tree, keep your appliance selected and click Troubleshooting.
   b. In the Troubleshooting section of the configuration pane, select Enable DXL tracing and, optionally, Write full message body into log.

4. Click Save Changes.

Gateway Anti-Malware with TIE rule set

The Gateway Anti-Malware with TIE rule set is a library rule set for integrating anti-malware filtering on Web Gateway with information retrieved from a TIE server.

<table>
<thead>
<tr>
<th>Library rule set – Gateway Anti-Malware with TIE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

The rule set contains the rules that are also contained in the default Gateway Anti-Malware rule set, as well the following rules, which are needed to enable the integrated filtering.

<table>
<thead>
<tr>
<th>TIE - Trusted reputations</th>
</tr>
</thead>
<tbody>
<tr>
<td>MediaType.EnsuredTypes at least one in list Executables AND TIE.Filereputation&lt;TIE Reputations&gt; greater than or equals 70 AND TIE.Filereputation&lt;TIE Reputations&gt; less than or equals 99 –&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>

The rule uses the MediaType.EnsuredTypes property to check whether a given web object is an executable file by looking it up in a list.

It also uses the TIE.Filereputation property to check whether the file reputation score for this object, which is retrieved from a TIE server, is between 70 and 99. This score means that the object is not considered malicious.

When the TIE.Filter module is called to retrieve the file reputation, it runs with the TIE.Reputation settings, as specified with the property.
If all parts of the criteria match, processing of the rule set stops and the rules that follow this rule in the rule set are skipped.

Skipping these rules means that the object is not scanned and filtered by the submodules of the Anti-Malware module on Web Gateway, which include the Gateway Anti-Malware (GAM) and Avira engines.

TIE - Unknown reputations

TIE.Filereputation<TIE Reputations> equals 50 AND TIE.Filereputation<TIE Reputations> greater than 0 → Continue

The rule uses the TIE.Filereputation property to check whether the file reputation score for this object, which is retrieved from a TIE server, equals 50, which means the reputation is not known.

When the TIE.Filter module is called to retrieve the file reputation, it runs with the TIE.Reputation settings, as specified with the property.

If the criteria matches, processing continues, which means the rule does not take any particular action on objects with unknown reputations.

This rule is not enabled by default.

TIE - Malicious reputations

TIE.Filereputation<TIE Reputations> less than or equals 30 AND TIE.Filereputation<TIE Reputations> greater than 0 → Block<TIE Reputation>

The rule uses the TIE.Filereputation property to check whether the file reputation score for this object, which is retrieved from a TIE server, is between 30 and 0, which means it is considered malicious.

When the TIE.Filter module is called to retrieve the file reputation, it runs with the TIE.Reputation settings, as specified with the property.

If both parts of the criteria match, 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.

This rule is not enabled by default.

Block if virus was found


The rule uses the MediaType.EnsuredTypes property to check whether a given web object is an executable file by looking it up in a list.

It also uses the Antimalware.Infected and Antimalware.Proactive.Probability properties to find out whether this object is infected by a virus or other malware and whether the probability that it is infected is between 60 and 80, which means it is likely that it is malicious.

When the Anti-Malware module is called to scan the object and rate its malware probability, it runs with the Gateway Anti-Malware with TIE settings, as specified with the properties.

These settings let the module use both its submodules, the Gateway Anti-Malware (GAM) engine and the Avira engine, and their methods to scan web objects.

If all parts of the criteria match, 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.

The rule uses another event to notify the TIE server that there is a high probability that the scanned object is malicious. Corresponding to this high probability grade, a low reputation score is sent to the TIE server.
Block if virus was found

**MediaType.EnsuredTypes** at least one in list Executables AND **Antimalware.Infected**<Gateway Anti-Malware with TIE> equals true AND **Antimalware.Proactive.Probability**<Gateway Anti-Malware with TIE> greater than or equals 80 AND **Antimalware.Proactive.Probability**<Gateway Anti-Malware with TIE> less than 90 –> Block< Virus Found> – **Statistics.Counter.Increment**("BlockedByAntiMalware",1)<Default> – TIE: Report File Reputation (15)

The rule uses the **MediaType.EnsuredTypes** property to check whether a given web object is an executable file by looking it up in a list.

It also uses the **Antimalware.Infected** and **Antimalware.Proactive.Probability** properties to find out whether this object is infected by a virus or other malware and whether the probability that is infected is between 80 and 90, which means it is very likely that it is malicious.

When the **Anti-Malware** module is called to scan the object and rate its malware probability, it runs with the Gateway Anti-Malware with TIE settings, as specified with the properties.

These settings let the module use both its submodules, the Gateway Anti-Malware (GAM) engine and the Avira engine, and their methods to scan web objects.

If all parts of the criteria match, 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.

The rule uses another event to notify the TIE server that there is a very high probability that the scanned object is malicious. Corresponding to this very high probability grade, a very low reputation score is sent to the TIE server.

Block if virus was found

**Antimalware.Infected**<Gateway Anti-Malware with TIE> 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 Anti-Malware with TIE` settings, as specified with the property.

These settings let the module use both its submodules, the Gateway Anti-Malware (GAM) engine and the Avira engine, 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.

The rule does not notify the TIE server of any scanning results.

**Dealing with a missing host header**

When the host header is missing from an ICAP request that is received on Web Gateway, additional measures can be required to configure anti-malware scanning for this request.

If you have only purchased a license for the McAfee scanning engine, the problem with the missing host header does not arise since this engine does not require the information that is provided by this header for scanning.

When a client of Web Gateway sends a request under the ICAP protocol, the host header can be missing from this request, which occurs, however, very rarely.

A request with no host header can be sent, for example, in the reqmod mode of ICAP communication. The GET portion of this request contains an empty URL, which means that this URL only consists of an entry for the HTTP protocol, which the ICAP request is embedded in. The URL then just looks as follows: `http://`.

**Importance of the host header**

When the Gateway Anti-Malware engine is involved in the scanning process on Web Gateway, it requires a URL to perform behavioral scanning as part of its scanning activities. The URL is used in the scanning, for example, to retrieve reputation scores and category information from the Global Threat Intelligence system.

The URL is assembled on Web Gateway from several sources, one of which is the host header in a request. It is then made available to the Gateway Anti-Malware engine. The URL cannot be assembled and made available, however, without retrieving information from the host header.

A missing host header therefore leads to an error in the scanning process when the Gateway Anti-Malware engine is involved in the usual way. Under the default rules, this error results in blocking the request, which means that it is not forwarded to the requested destination. The error is logged in the mwg-antimalware log.

**Combined use of anti-malware engines**

For scanning web traffic, the Gateway Anti-Malware engine relies in parts on another scanning engine, which is known as McAfee engine. A reduced range of scanning activities can also be performed by the McAfee engine alone, but only the combined use of the two engines ensures the anti-malware protection that we recommend.

Whether both engines are available on Web Gateway depends on whether you have purchased a license for the Gateway Anti-Malware engine, which also covers use of the McAfee engine, or a license for the McAfee engine only.
Solving the host header problem

There are several ways to solve the problem when a host header is missing from an ICAP request.

- Configure the ICAP client to send a host header.
  
  This solution is not applied on Web Gateway, but on the client system that sent the incomplete request. The request might have been sent without a host header due to an error within the client configuration.
  
  For more information, refer to documentation that explains the ICAP protocol.

- Create rules for anti-malware filtering with full and reduced use of the Gateway Anti-Malware engine.
  
  You can perform scanning with a reduced use of the Gateway Anti-Malware engine that does not require the processing of information from a host header.
  
  The rule set for anti-malware filtering then includes:
  
  - A rule for performing the default scanning process with full use of the Gateway Anti-Malware engine if a request includes a host header
  - A rule for performing a scanning process with reduced use of the Gateway Anti-Malware engine if a request does not include a host header
  
  For more information about these two rules, see the Rules for anti-malware filtering with full or reduced use of the Gateway Anti-Malware engine subsection.

- Create a rule that adds a host header.
  
  You can add a rule that sets a value for the host header and place it before the rule that controls anti-malware scanning. When this second rule is executed, the host header value is found by the rule engine and scanning can be performed making full use of the Gateway Anti-Malware engine.
  
  The rule provides the host header value using an event that sets the URL.Host property. If you know that requests are usually received from a particular host, you can set the property to the value for this host.
  
  If you do not know such a host, you can set the property to a dummy value. Setting the property in this way is sufficient for letting the scanning process make full use of the Gateway Anti-Malware engine. Inappropriate host information can, however, have an impact on the anti-malware filtering results, which might include an increased number of false positives.
  
  For more information about the rule, see the Rule for adding a host header subsection.

Rules for making full or reduced use of the Gateway Anti-Malware engine

The following are sample rules for performing anti-malware filtering with full or reduced use of the Gateway Anti-Malware engine, depending on whether a host header is sent with a request or missing from it.

When creating these rules, you can use the rule Block if virus was found in the default Gateway Anti-Malware rule set as a starting point. After creating and enabling these rules, the default rule must be deleted.

The first rule blocks a request that includes a host header if scanning the request results in detecting an infection by a virus or other malware.

When the rule engine processes the rule, it calls the Anti-Malware module to provide a value for the AV.Infected property. The module runs with default settings, which means full use of the Gateway Anti-Malware engine is made in the scanning process that is performed to provide the property value.

Name

Scan with full use of the Gateway Anti-Malware engine

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
</table>

When creating these rules, you can use the rule Block if virus was found in the default Gateway Anti-Malware rule set as a starting point. After creating and enabling these rules, the default rule must be deleted.
The second rule blocks a request that does not include a host header if scanning the request results in detecting an infection by a virus or other malware.

When the rule engine processes the rule, it calls the Anti-Malware module to provide a value for the AV.Infected property. The module does not run with default settings, but with new settings that let the scanning process be performed with reduced use of the Gateway Anti-Malware engine.

The new settings differ from the default settings in that the option Enable mobile code scanning is disabled.

**Rule for adding a host header**

The following is a sample rule for adding a host header to an ICAP request that was sent with this header missing.

**Configure settings for reduced use of the Gateway Anti-Malware engine**

Configure an option in the settings for anti-malware filtering to achieve a reduced use of the Gateway Anti-Malware engine. This reduced use can be required if a request does not contain a host header.

**Task**

1. Create new settings for anti-malware filtering, based on the default settings, and give them a suitable name, for example, **Reduced use of Gateway Anti-Malware engine**.

2. Within the new settings, expand **Advanced Settings for McAfee Gateway Anti-Malware**.

3. Deselect **Enable mobile code scanning**.

4. Click **Save Changes**.

You can now insert the new settings in a rule for performing anti-malware filtering with reduced use of the Gateway Anti-Malware engine.

For more information about how to create new settings, see the **Create action and module settings** section of the **Settings** chapter.
**Media stream scanning**

Media streams can be scanned on Web Gateway chunk-by-chunk, which allows users to see or hear downloaded streaming media faster, as they do not have to wait until a stream has been scanned completely. This scanning method is performed by the Media Stream Scanner, which is provided by the Gateway Anti-Malware engine. Streaming media is scanned and delivered chunk-by-chunk to the client that requested the download. If an infection is detected in a chunk, the download stops, and this chunk and the rest of the streaming media are not delivered.

The scanning that is performed by the Media Stream Scanner uses the proactive functions of the Gateway Anti-Malware engine. The Avira engine, which can also be configured to scan web objects for infections by viruses and other malware, is not involved when the Media Stream Scanner is active.

The scanner is started by an event of a rule in the **Gateway Anti-Malware** rule set of the default rule set system. The rule applies if the Stream Detector module finds that a web object that was received on Web Gateway in response to a download request is streaming media.

Processing of the rule set stops and the remaining rule in the rule set, which also lets web objects be scanned for infections by viruses and other malware, is not processed.

If a web object is not recognized by the Stream Detector as streaming media, the rule does not apply, processing continues with the remaining rule, and the web object is scanned according to the settings that are configured for this rule.

**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**. When a request has been received on the appliance, it is moved to this queue by a working thread of the proxy module. It remains 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 are used by the modules to execute scanning activities, are referred to as **anti-malware working threads** or simply as **AV threads**.

When configuring the anti-malware queue, you can specify the following:

- Number of available anti-malware working threads
- Size of the anti-malware queue
- Maximum time for requests and responses to stay in the queue

Moving requests and responses to the anti-malware queue is a solution to avoid load peaks occurring over a short period of time. Permanent overloading should be addressed by other measures.

**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 10-1  Global Anti-Malware Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of threads for AV scanning</strong></td>
<td>Sets the 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.</td>
</tr>
<tr>
<td><strong>Use at least as many AV threads as the number of CPU cores available</strong></td>
<td>When selected, the number of AV threads use for scanning activities is at least the same as the number of available CPU cores.</td>
</tr>
<tr>
<td><strong>Maximum number of jobs in the queue</strong></td>
<td>Limits the number of requests or responses that can be moved to the anti-malware queue as jobs for the scanning modules.</td>
</tr>
<tr>
<td><strong>Number of seconds a scanning job stays in the queue before being removed</strong></td>
<td>Limits the time (in seconds) that elapses before a request or response is removed from the anti-malware queue if it has not been forwarded for scanning.</td>
</tr>
</tbody>
</table>

**URL filtering**

URL filtering ensures that the users of your network cannot access web objects that are considered a risk for web security or are not allowed for other reasons.

The filtering process uses blocking lists, category information, and reputation scores for the URLs of web objects and blocks or allows access accordingly.

The process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- A whitelist and various blocking lists are used by rules to let some web objects skip URL filtering and block others.
- The URL Filter module, which is called by particular rules, retrieves information on URL categories and web reputation scores from the Global Threat Intelligence service.
A default process for URL filtering is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure URL filtering, you can work with:

- **Key elements of rules** — After clicking the default URL filtering rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

### Filtering rules

The rules that control the URL filtering process are usually contained in one 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.

When the default rule set system is implemented, a rule set for URL filtering is included. Its name is **URL Filtering**.

### Whitelist and blocking lists

A whitelist is used by a whitelisting rule to let some URLs skip the blocking rule, which means there is no filtering for these URLs.

Since a URL filtering rule set controls only URL filtering, multiple whitelists for several types of objects are not needed in the filtering process, in contrast to virus and malware filtering.

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 is also known as the URL Filter engine. It retrieves information on URL categories and reputation scores from the Global Threat Intelligence™ service that is provided 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 key elements for URL filtering**
Configure key elements of the rules for URL filtering to adapt important parts of the filtering process to the requirements of your web security policy.

**Task**
2. On the rule sets tree, select the URL Filtering rule set.
   - Key elements of the rules for the filtering process appear in the configuration pane.
3. Configure the key elements as needed.
4. Click Save Changes.

**Configure URL filtering using the complete rules view**
You can configure URL filtering to adapt this process to the needs of your network.

To configure URL filtering, you can work with the key elements view or the rules view.

**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
     - 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 settings for 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**
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.

Best practices - Using URL properties to whitelist web objects

URL properties, such as URL, URL.Host, URL.Host.BelongsToDomains, and others, can be used in the criteria of rules to whitelist web objects.

When a web object is whitelisted, users are allowed to access it, for example, to view a web page or download a file. Whitelisting rules are inserted into appropriate rule sets within the rule set system of Web Gateway. They usually stop further rule processing with regard to the current request for accessing a web object to prevent other rules from blocking this access.

Different URL properties can be used for different kinds of whitelisting. To allow access to an individual web object, for example, to ensure users can download a particular file, the URL property is best used together with a list that contains the full URL for this file.

The following examples explain which URL properties are best used for different kinds of whitelisting and how to do it.

In addition to this, some tips and examples are given regarding the:

- Values that different URLs are set to when a sample URL is processed that has been sent to Web Gateway in a request for web access
- Use of the two operators is in list and matches in list in the criteria of a rule
- Good and bad entries in the lists that are used with different URL properties

Whitelisting individual web objects – URL

**Goal**

Allow users to access individual web objects.

*For example, download the file Stinger.exe, which can be accessed using the URL http://download.mcafee.com/products/mcafee-avert/Stinger/Stinger.exe.*

**How to do it**

Use the URL string property with a list of full URLs in the criteria of a rule.

The rule could, for example, be configured as follows:

*URL is in list URLWhiteList* → Stop Rule Set
If you add the URL `http://download.mcafee.com/products/mcafee-avert/Stinger/Stinger.exe` to the list `URLWhiteList`, the file `Stinger.exe` is whitelisted when the rule is processed.

In a similar way, you can block access to the file using the following rule from the default URL Filtering rule set:

```
URL matches in list URLBlockList -> Block
```

If you add the URL in question to the list `URLBlockList`, the file is blocked when the rule is processed.

If the `matches in list` operator is used instead of `is in list`, expressions containing wildcards can be entered into the list that is used by the property. The property can then also be used to whitelist multiple web objects.

However, if all web objects provided by a particular host should be whitelisted, this can be achieved more easily using the `URL.Host` property.

### Whitelisting hosts – `URL.Host`

**Goal**

Allow users to access the web objects that are provided on particular hosts.

For example, download the file `Stinger.exe` or any other file that is provided on the host `download.mcafee.com`.

**How to do it**

Use the `URL.Host` string property with a list for host names in the criteria of a rule.

A rule that the `URL.Host` property is used in could, for example, be configured as follows:

```
URL.Host is in list HostWhiteList -> Stop Rule Set
```

If you add the host `download.mcafee.com` to the list `HostWhiteList`, all web objects that are provided by this host are whitelisted when the rule is processed.

If the `matches in list` operator is used instead of `is in list`, expressions containing wildcards can be entered into the list that is used by the property. The property can then also be used to whitelist multiple hosts.

However, if all hosts within a particular domain should be whitelisted, this can be achieved more easily using the `URL.Host.BelongsToDomains` property.

### Whitelisting domains – `URL.Host.BelongsToDomains`

**Goal**

Allow users to access the web objects that are provided within particular domains.

For example, download the file `Stinger.exe` and any other file that is provided by the host `download.mcafee.com`, as well as any other downloadable file provided by any other host within the domain `mcafee.com`.

**How to do it**

Use the `URL.Host:BelongsToDomains` Boolean property with a list of domain names in the criteria of a rule.

The rule could, for example, be configured as follows:

```
URL.Host:BelongsToDomains("Domain List") equals true -> Stop Rule Set
```

If you add the domain `mcafee.com` to the list `Domain List`, all web objects within this domain are whitelisted when the rule is processed.

The list `Domain List` is configured as a parameter of the `URL.Host:BelongsToDomains` property, which is of the Boolean type.
When, for example, the URL http://download.mcafee.com/products/mcafee-avert/Stinger/Stinger.exe is processed, the value of the property (true or false) depends on whether the mcafee.com domain has been entered into the list Domain List or not.

The following example shows which entries in the list Domain List lead to a match when the property is used for whitelisting:

mcafee.com
dell.com
k12.ga.us
twitter.com
xxx

Then the criteria:

URL.Host.BelongsToDomains("Domain List") equals true

matches for the following URLs:

https://contentsecurity.mcafee.com
https://my.mcafee.com
http://my.support.dell.com
http://www.dekalb.k12.ga.us
http://twitter.com
http://www.twitter.com
any.site.xxx

but not for:

https://www.mymcafee.com
http://www.treasury.ga.us
http://malicioustwitter.com

Using the URL.Host.BelongsToDomains property also avoids the effort of creating more complicated solutions to achieve the same, for example:

• Using two entries in a list of wildcard expressions, such as:
  
  twitter.com
  *
twitter.com

• Using a single, complex entry in a list of wildcard expressions, such as:
  
  regex((.*\.|\.)twitter\.com)

**Property values for a sample URL**

When the sample URL http://www.mcafee.com/us/products/web-gateway.aspx is processed, the URL properties below are set to different values as follows.
<table>
<thead>
<tr>
<th>Property</th>
<th>Value for sample URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL.Host</td>
<td><a href="http://www.mcafee.com">www.mcafee.com</a></td>
</tr>
<tr>
<td>URL.Host.BelongsToDomain</td>
<td>true or false</td>
</tr>
<tr>
<td></td>
<td>In the list that is configured as a parameter of this property, the following</td>
</tr>
<tr>
<td></td>
<td>would have to be entered for the domain: mcafee.com.</td>
</tr>
<tr>
<td>URL.FileName</td>
<td>web-gateway.aspx</td>
</tr>
<tr>
<td>URL.Path</td>
<td>/us/products/web-gateway.aspx</td>
</tr>
<tr>
<td>URL.Protocol</td>
<td>http</td>
</tr>
</tbody>
</table>

**Use of operators for different types of matches**

It makes an important difference whether the *is in list* or *matches in list* operator is used in the criteria of a rule.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is in list</td>
<td>Requires an exact string match. If there are wildcard characters in a list</td>
</tr>
<tr>
<td></td>
<td>entry, they are interpreted as literal strings.</td>
</tr>
<tr>
<td>matches in list</td>
<td>Allows and evaluates wildcards in list entries.</td>
</tr>
</tbody>
</table>

**Good and bad entries in lists for URL properties**

Entries in the lists that are used by the different URL properties can be good are bad, according to how they fit in with the intended use of a property. The following are examples of good and bad list entries.
<table>
<thead>
<tr>
<th>URL property</th>
<th>Good and bad list entries</th>
</tr>
</thead>
</table>
| **URL with *is in list* operator** | **Good**  
The full URL is entered, as it is required for this property. No wildcards are specified, as these are not evaluated when the *is in list* operator is used.  
**Bad**  
The entry does not specify the full URL, as the protocol information, http://, is not included. |
| **URL with *matches in list* operator** | **Good**  
http://www.mcafee.com/*  
This entry contains a wildcard for allowing access to any web object provided by the host www.mcafee.com, which is appropriate when the *matches in list* operator is used.  
![The entry will not match for http://mcafee.com/](regex(http|ps)://(/.*\.|\.|\.?\w+e.com|v.+|v?))  
This entry is more complex, as it uses regular expressions. When matched, it allows access, under the HTTP or HTTPS protocol, to any web object within the domain mcafee.com and its subdomains.  
regex(http|ps)://(/.*\.|\.|\.?\w+e.com|co.us|co.us)(/.*|/?)  
This entry is the same as the previous, but shows how other top-level domains, such as .com or .co.us, can be whitelisted.  
**Bad**  
*.mcafee.com*  
The entry does not exclude unwanted matches, for example, a match for the URL http://malicious-download-site.cc/malicious-file.exe?url=www.mcafee.com. |
| **URL.Host with *is in list* operator** | **Good**  
www.mcafee.com  
A host name is entered, which fits in with the intended use for this property. No wildcards are specified, which is appropriate when the *is in list* operator is used.  
**Bad**  
mcafee.com  
The entry specifies a domain name (mcafee.com), whereas the value of the property is a host name (www.mcafee.com if, for example, the URL http://www.mcafee.com/us/products/web-gateway.aspx is processed).  
No match will be produced this way.  
*.mcafee.com  
The entry contains a wildcard, which is not evaluated when the *is in list* operator is used.  
*.mcafee.com/us*  
The entry includes path information (/us), which does not fit in with the intended use of the property.  
In addition to this, a wildcard is specified, which is not evaluated when the *is in list* operator is used. |
### URL property

#### URL.Host with matches in list operator

**Good**

- `*.mcafee.com`
  
The entry matches for on any host within the domain mcafee.com, but not for mcafee.com itself.
  
  `regex((.*\.|\.|\.)mcafee.com)`
  
The entry uses regular expressions to whitelist the domain mcafee.com and any of the hosts within it.

**Bad**

- `*.mcafee.com*`
  
The entry does not exclude unwanted matches, for example, http://www.mcafee.com.malicious-download-site.cc/.

- `*.mcafee.com/us*`
  
The entry includes path information (/us), which does not fit in with the intended use of the property.

### URL.HostBelongsToDomains

**Good**

- `mcafee.com` entered in the list Domain List, which is configured as a parameter of the property.
  
The entry matches for the mcafee.com domain and all hosts within it, for example, www.mcafee.com or secure.mcafee.com.

- `www.mcafee.com`
  
The entry does not specify a domain, but is valid. It only whitelists the host www.mcafee.com.

**Bad**

- `*.mcafee.com*`
  
The entry contains a wildcard, which does not fit in with the intended use of the property.
  
The property was rather developed to avoid the effort of using wildcards in list entries. Instead it requires an exact domain match, for example, a match for mcafee.com.

### 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 use 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.

URL filtering using the Dynamic Content Classifier

URLs can be categorized for filtering by the Dynamic Content Classifier.

The Dynamic Content Classifier (DCC) is another source of category information with regard to URLs, in addition to the local database and the Global Threat Intelligence service.

You can configure use of the Dynamic Content Classifier when lookups for URL category information involving the other two sources yield no results.

Configure use of the Dynamic Content Classifier

You can configure use of the Dynamic Content Classifier for detecting URL categories when other methods of detection yield no results.

Task


2. On the rule sets tree, select a rule set with rules for URL filtering.
   In the default rule set system, this is, for example, the URL Filtering rule set.
   The rules appear in the settings pane.

3. Make sure Show details is selected.

4. Select the rule for handling URL categories that you want to configure use of the Dynamic Content Classifier for.
   In the URL Filtering rule set, this is, for example, the rule Block URLs whose category is in Category BlockList.

5. Click the settings of the URL Filter module in the rule criteria.
   In the sample rule, these are the Default settings in the criteria URL.Categories <Default> at least one in list Category BlockList.
   The Edit Settings window opens. It provides the settings of the URL Filter module.

6. Under Rating Settings, make sure Enable the Dynamic Content Classifier if GTI web categorization yields no results is selected.

7. [Optional] Edit the list of URL categories the Dynamic Content Classifier should detect.
   a. Above the list Categories that will be dynamically detected, click the Edit icon.
      The Edit window opens.
   b. Under DCC category, expand the Supported Categories folder.
Select or deselect URL categories as needed.

Click OK.

The Edit window closes and the selected categories appear on the list.

You can remove a URL category from the list by clicking the Delete symbol and confirming in the window that opens.

8 Click OK to close the Edit Settings window.

9 Click Save Changes.

The Dynamic Content Classifier is now involved in detecting whether a URL that is submitted in a request for web access falls into one of the configured URL categories.

Using your own URL filter database

URL filtering can be performed using information that is retrieved from a database of your own.

URL filtering on a Web Gateway appliance uses information about the categories that URLs fall into and the web reputation scores that are assigned to them. This information is retrieved from the local URL filter database, the Global Threat Intelligence system, or the Dynamic Content Classifier, depending on how the settings of the module for URL filtering are configured.

The information in the local database is the result of storing categories and web reputation scores there after they have been determined for particular URLs by the Global Threat Intelligence system. When a lookup in the local database yields no results, the other two information sources can additionally be used.

Instead of the local database, you can use a database of your own, containing information on URL categories and web reputation scores. To replace the local database, you need to specify the URL of the server that your database resides on when configuring the Central Management settings.

You can use your own database as the source that is searched first to retrieve URL filtering information, but also disable the other two sources and restrict the filtering process to using the information stored in your database.

Configure use of your own URL filter database

To retrieve URL filtering information from a database of your own, configure the use of this database as part of the Central Management settings.

Task

1 Select Configuration | Appliances.

2 On the appliances tree, select the appliance that should use your database information and click Central Management.

3 Scroll down to Advanced Update Settings.

4 In the Enter a special custom parameter for an update server field, enter the URL of the server that your database resides on.

5 Click Save Changes.

When database information is used to filter URLs on the appliance, it is not retrieved from the local database, but from your own database.

You can additionally disable other sources of URL filtering information to restrict the filtering process to the information stored in your own database.
Restrict URL filtering to using database information
To use only database information for URL filtering, disable use of the Global Threat Intelligence system and the Dynamic Content Classifier.
If you configured the use of your own URL filter database, filtering information is retrieved only from this database.

Task
1. Select Policy | Settings.
2. Under Engines | URL Filter, select the URL Filter settings you want to disable information sources for.
3. Under Rating Settings, deselect the following two checkboxes one after another:
   - Enable the Dynamic Content Classifier if GTI web categorization yields no result
   - Use online GTI web reputation and categorization services if local rating yields no result
4. Click Save Changes.

URL filtering using an IFP proxy
URL filtering can be performed on requests to web access submitted under the IFP protocol.
To perform URL filtering on such requests, you need to:
- Set up an IFP proxy.
- Implement suitable filtering rules.
Filtering activities for IFP requests are displayed on the dashboard of the user interface. Connection tracing can also be performed for these activities.

Setting up an IFP proxy
To process and filter requests for web access that users submit from their client systems under the IFP protocol, the proxy functions of the appliance must be appropriately configured. An IFP proxy must be set up that intercepts these requests and makes them available for URL filtering.

To set up the proxy, you need to specify a number of settings on the user interface under Configuration | Proxies.
These settings include:
- Enabling or disabling the proxy
- List of proxy ports, specifying for each proxy:
  - IP address and port number
  - Message mode (Indicates whether a block message is sent as a redirect or as normal message under the IFP protocol)
- Maximum number of concurrent IFP requests
  Using this setting, you can prevent an overloading of the IFP proxy.

Rules for filtering IFP requests
There is no default or library rule set for controlling the process of filtering IFP requests. However, you can create a rule set of your own and also make use of the IFP proxy functions in existing rule sets.

When creating a rule set for filtering IFP requests, you need to specify use of the IFP protocol as the rule set criteria to ensure the rule set is applied to requests that are submitted under this protocol. This is achieved by including the Connection.Protocol property in the criteria and configuring the IFP protocol as its operand.
As the IFP protocol covers only requests, you can exclude filtering responses and embedded objects as activities that the rule set should apply to.

The rules in the rule set can be the same as in the default URL Filtering rule set.

**Best practice:** If you want to perform URL filtering only for requests sent under the IFP protocol, delete the default URL Filtering rule set and use only the IFP filtering rule set that you have created in the way described here.

Using the IFP proxy functions in existing rule sets can be an option, for example, if you have authentication implemented for requests submitted under various other protocols and want to add authentication for IFP requests.

The Authentication Server (Time/IP-based Session) library rule set contains an embedded rule set with rules that check whether there is already an authenticated session for a client that a request is received from. Otherwise a rule redirects a request to the authentication server.

The embedded rule set covers protocols such as HTTP or HTTPS. Using the `Connection.Protocol` property, you can extend the criteria to include the IFP protocol.

**Restrictions for IFP filtering**

When using an IFP proxy for filtering URLs, you should be aware of the following restrictions:

- **Limited use of SafeSearch Enforcer**

  When performing IFP filtering, you the SafeSearch Enforcer will only work for filtering search requests that are carried out using Google.

  The reason for this is that only Google uses URLs for submitting the search criteria while all other search providers use cookies. However, cookies cannot be processed by the IFP proxy on an appliance.

- **HTTP proxy required for some functions**

  An HTTP proxy must be set up in addition to the IFP proxy if you want to do the following:

  - Redirect IFP requests that are blocked due to a filtering rule to a blocking page to let a block message appear on the client of the user who sent the request.

  - Authenticate users on the appliance by having their credentials verified on the internal authentication server.

  - Restrict web usage of users by implementing the Time Quota library rule set.

**IFP filtering activities on the dashboard**

The dashboard on the user interface provides information on several IFP filtering activities.

- **Number of IFP requests processed**

  This information is shown under Web Traffic Summary | Requests per protocol.

- **Domains that access to was requested most often (counting the number of requests)**

  Among these requests can be such that were submitted under the IFP protocol.

  This information is shown under Web Traffic | Top Level Domains by Number of Requests.

- **Websites that were most often the destinations of requests (counting the number of requests)**

  Among these requests can be such that were submitted under the IFP protocol.

  This information is shown under Web Traffic | Destinations by Number of Requests.
**Connection tracing for IFP filtering activities**

Connection tracing can be performed for filtering IFP requests.

When connection tracing is enabled, connection tracing files are created and stored. They can be accessed on the user interface under the **Troubleshooting** top-level menu.

**Configure the IFP Proxy settings**

You can configure the IFP proxy settings to set up a proxy that enables the processing of requests for web access submitted under this protocol.

**Task**

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

2. On the appliances tree, expand the appliance you want to configure the IFP proxy settings for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3. On the settings pane, scroll down to the **IFP Proxy** section.

4. Configure the settings in this section as needed.

5. Click **Save Changes**.

**Create a rule set for filtering IFP requests**

You can create a rule set with rules that filter requests for web access submitted under the IFP protocol.

**Task**

1. Select **Policy** | **Rule Sets**, then click **Add** and select **Rule Set**.

   The **Add New Rule Set** window opens.

2. In the **Name** field, enter a suitable name for the rule set, for example **Filter IFP Requests**.

3. Under **Applies to**, deselect **Responses** and **Embedded Objects**.

4. Under **Apply this rule set**, select **If the following criteria is matched**.

5. Configure the rule set criteria.

   a. Under **Criteria**, click **Add** and select **Advanced criteria**.

      The **Add Criteria** window opens.

   b. From the properties list, select **Connection.Protocol**.

   c. From the operators list, select **equals**.

   d. In the input field for operands, type **IFP**.

   e. Click **OK**.

      The **Add Criteria** window closes and the criteria appears in the **Criteria** field.

6. Click **OK**.

   The **Add New Rule Set** window closes and the new rule set appears on the rule set tree.

When the rule set has been created, you need to insert rules for URL filtering into it. You can, for example, copy rules from the default URL Filtering rule set and adapt them as needed.
Modify an authentication rule set to include the IFP protocol
You can include the IFP protocol in the criteria of an authentication rule set to enable authentication for requests that are submitted under that protocol.

Task
1 Import an authentication rule set from the library.
   a Select Policy | Rule Sets, then click Add and select Top Level Rule Set.
      The Add Top Level Rule Set window opens.
   b Click Import rule set from Rule Set Library.
      The Add from Rule Set Library window opens.
   c From the Rule Set Library list, select the Authentication (Time/IP-based Session) rule set.
   d In the Import conflicts area, select the conflict that is listed and under Conflict Solution choose a conflict-solving strategy.
   e Click OK.
      The Add from Rule Set Library window closes and the rule set appears on the rule set tree.

2 Expand the rule set and select the embedded Check for Valid Authentication Session rule set.
   The criteria and rules of the embedded rule set appear on the settings pane.

3 Click Edit. The Edit Rule Set window opens.

4 Modify the rule set criteria.
   a Under Criteria, click Add and select Advanced criteria.
   b From the properties list, select Connection.Protocol.
   c From the operators list, select equals.
   d In the input field for operands, type IFP.
   e Click OK.
      The Add Criteria window closes and the criteria appears in the Criteria field.
   f Under Criteria combination remove the closing parenthesis after the letter e and insert one after d.

5 Click OK.
   The Edit Rule Set window closes.

6 Click Save Changes.

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, when these types are not allowed under your web security policy. This way you can, for example, prevent your users from consuming too many resources.
The media type filtering process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- A blocking list is used by a rule to block access to media that belong to particular types.

A default process for media type filtering is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure media type filtering, you can work with:

- **Key elements of rules** — After clicking the default Media Type Filtering rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can expand the Media Type Filtering rule set on the rule sets tree, which lets the nested Upload Media Types and Download Media Types rule sets appear.

  Clicking either of them lets you view their default rules for the filtering process completely. You can configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

### Filtering rules

The rules that control the media type filtering process are usually contained in one media type filtering rule set. It can have two nested rule sets with rules for filtering media types that are uploaded to and downloaded from the web.

When the default process is implemented, a rule set for media type filtering with two nested rule sets is included. The name of the nesting rule set is Media Type Filtering, those of the nested rule sets are Upload Media Types and Download Media Types.

A media type filtering rule can use a list of media types. It can also rely on the use of a suitable property in its criteria, such as the MediaType.IsAudio or MediaType.IsVideo properties.

### Blocking list

A blocking list is used by a rule for blocking media that belong to particular types. There can be a blocking list for media that should not be uploaded from within your network to the web, as well as one for media that should not be downloaded from the web to your network.

### Configure key elements for media type filtering

Configure key elements of the rules for media type filtering to adapt important parts of the filtering process to the requirements of your web security policy.

**Task**

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

2. On the rule set tree, select the **Media Type Filtering** rule set.

   Key elements of the rules for the filtering process appear in the configuration pane.
3 Configure the key elements as needed.

4 Click Save Changes.

**Configure media type filtering using the complete rules view**

You can configure media type filtering to adapt this process to the needs of your network. To configure URL filtering, you can work with the key elements view or the rules view.

**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
     
     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.

**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 200*
  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 201*
  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**

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.

**Media Type Filtering rule set**

The Media Type Filtering rule set is the default rule set for media type filtering.

<table>
<thead>
<tr>
<th>Library rule set – Media Type Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

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**

Mediatypeensuredtypes at least one in list Upload Media Type Blocklist \(\rightarrow\) Block\{Media Type (Block List)\} \(\rightarrow\) Statistics.Counter.Increment ("BlockedByMediaFilter", 1)<Default>

The rule uses the Mediatypeensuredtypes 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**

Mediatypeensuredtypes at least one in list Download Media Type Blocklist \(\rightarrow\) Block\{Media Type (Block List)\} \(\rightarrow\) Statistics.Counter.Increment ("BlockedByMediaFilter", 1)<Default>

The rule uses the Mediatypeensuredtypes 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 application names and reputation scores and blocks access accordingly. Filtering can also be applied to individual functions of applications.

The following elements are involved in this process:

- Filtering rules that control the process
- Application lists that are used by rules to block applications
- Application system lists that are updated in intervals

Update status and statistics of the application 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 and individual functions of applications using the following two methods:

- Block applications and individual functions that are on a list
- Block applications that are assigned a particular risk level

To block applications and individual functions according to a list, the `Application.Name` property is used.

The value of this property is the name of an application or an individual function of an application that appears in a request sent by a user who wants to access the application or application function. 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
Application.Name is in list Unwanted Applications
Action
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
Application.IsMediumRisk equals true OR Application.isHighRisk equals true
Action
Block<Application Blocked>
```

Both methods rely on the application system lists. Only applications and application functions that are on these lists can appear on a list that is used by an application filtering rule.

The risk levels for applications and application functions are also those that are shown on the application system lists.

For logging purposes, there are the `Application.ToString` 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 performed 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.

**Blocking lists**

Blocking lists are used by rules to block access to applications that are requested by users. The rules in the library rule set include lists 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 must take them from the application system list.
In the same way, you can create and edit lists with names of application functions.

**Application system lists**
The applications and application functions that can be blocked by application filtering rules appear on lists, which are provided by the appliance system and updated in intervals.

You can view these lists by expanding the *Application Name* folder under *System Lists* on the lists tree of the *Lists* tab. This folder contains a number of subfolders for different types of applications, for example, *File Sharing* or *Instant Messaging*.

A subfolder contains a list of applications, providing the following information for each of them:

- Application name (or application name with application function)
- Comment
  - Risk level
- Description of the application (or application function)

A function of an application appears in parentheses after the application name, for example, *Orkut(Orkut Chat)*. If you include an application function in the list of a blocking rule, only this function is blocked, not the complete application.

The following is an example of an entry for an application in a system list:

*MessengerFX* | *Risk: Minimal: A web-based instant messaging service*

The next example shows an entry for an application function:

*Orkut(Orkut Chat)* | *Risk: High: Allows users to send instant messages.*

**Application filtering information on the dashboard**
The dashboard provides the following information on application filtering:

- Update status of the application list
- Statistics on applications and application functions 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
   - Create lists of your own and use them instead of or in addition to the existing lists
   - 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.

**Create a list for application filtering**

You can create a list for use in an application filtering rule and fill it with entries for applications or individual functions of applications that should be blocked.

**Task**

1 Select Policy | Lists and click the Add icon.

The Add List window opens.

2 Configure general list settings.
   a In the Name field, type a name for the list, for example, Unwanted Applications.
   b From the Type list, select Application Name.
   c [Optional] Click the Permissions tab and configure who is allowed to access the list.
   d [Optional] In the Comments field, type a plain-text comment on the list.

3 Click OK.

The Add List window closes and the list appears on the list tree under Custom Lists | Application Name.

4 Select the list and, above the settings pane, click the Edit icon.

The Edit window opens with a collection of folders that contain application names.

5 Fill the list with entries for applications or individual functions of applications.
   a Expand a folder that contains an application or application function that you want to add to the list, for example, Instant Messaging Web Applications.
   b Select an application or application function, for example, MessengerFX or Orkut(Orkut Chat).

   You can select multiple applications or application functions at once, you can select items from multiple folders at once, and you can select complete folders.

   c Click OK.

   The Edit window closes and the selected applications and application functions appear on the list.

   You can also add a complete folder and afterwards delete the entries for applications or application functions that you do not want to include.

6 Click Save Changes.

You can use the list you created in the criteria of an application filtering rule, for example, to let the criteria match if the name of an application or application function that access is requested to appears on the list.
Modify the risk level in an application filtering rule

You can modify the risk level in a rule that filters applications according to the risk they present to web security, for example, from high to medium. This increases web security because a blocking action can then be triggered even if an application is only a medium risk.

Before you begin
The following procedure assumes that you have imported the Application Control rule set from the library.

Task
   The Add New Rule Set window opens.
2. Expand the Application Control rule set, then expand the nested Block Applications in Request Cycle rule set.
   The general settings and rules of the nested rule set appear on the settings pane.
3. Make sure Show details is selected.
4. Select the rule Block web applications with high risk and click Edit.
   The Edit Rule window opens.
5. Under Steps, select Rule Criteria and in the Criteria section, select the upper part of the complex criteria (the one that uses the Application.IsHighRisk property), then click Edit.
   The Edit Criteria window opens with the Application.IsHighRisk property selected in the properties list.
6. From the properties list, select Application.IsMediumRisk.
7. Click OK.
   The Edit Criteria window closes and the modified criteria appears in the Criteria section.
8. Click Finish.
   The Edit Rule window closes and the rule with the modified criteria appears on the settings pane.
9. Click Save Changes.

Application Control rule set
The Application Control rule set is a library rule set for application filtering.

<table>
<thead>
<tr>
<th>Library rule set – Application Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Criteria – Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.ToString* 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.

<table>
<thead>
<tr>
<th>Nested library rule set – Block Applications in Response Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycle – Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rule:

**Applications to be looked for in response cycle**

*Application.Name is in list 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.ToString` 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 web objects of this media type are detected when they are received on Web Gateway and handled according to the configured rules.

When virus and malware filtering is implemented on Web Gateway, web objects that are sent to it are scanned for infections. To achieve a comprehensive scanning result, the web object needs to be scanned completely.

However, streaming media is never "complete", so if the usual scanning method is applied to it, it will not deliver a result, as it would for other, non-streaming media.

Processing streaming media would also be delayed endlessly, as the scanning process would never finish.

This means that once a web object has been detected to be streaming media, you can block it to prevent the users of your network from accessing web objects that have not been scanned for infections.

Or you let streaming media skip virus and malware scanning and allow your users to access media of this type unscanned.

The following elements on Web Gateway are involved in the filtering process:

- Filtering rules that control the process
- A module that calculates the probability for web objects that they are streaming media

  The module sets the value of a suitable property to `true` if the probability for a web object to be streaming media reaches or exceeds a configured value.

Streaming media filtering is usually applied in the response cycle of the filtering process to deal with streaming media sent by web servers in response to user requests.

**Rules for streaming media detection**

To block or allow 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 would be blocked by the following rule.

**Name**

**Block access to streaming media**

**Criteria**

**Action**
StreamDetector.IsMediaStream<Streaming Detection> equals true  –>  Block<Streaming Media Blocked>

It would be allowed by the following rule:

Name
Allow access to streaming media
Criteria  Action
StreamDetector.IsMediaStream<Streaming Detection> equals true  –>  Continue

The value of the StreamDetector.IsMediaStream property is provided by the Stream Detector module.

Streaming media filtering is not performed by default on Web Gateway. If you want to have it done, you need to create a rule like the ones described above.

**Best practice:** 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.

The default Gateway Anti-Malware rule set contains a rule that lets streaming media skip virus and malware filtering. In this rule set, the skipping rule is placed before the rule that lets web object be scanned by the Anti-Malware scanning module.

**Additional properties for streaming media filtering**

When the StreamDetector.IsMediaStream 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.IsMediaStream property is the name of the rule that matched.

You can use these additional properties in rules that record information in log file entries.

**Module for streaming media 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 Media Detection. The settings include the minimum probability that must be reached for a web object to be considered as 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 media detection module**

You can configure the module that calculates the streaming media probability for a given web object to adapt it to the requirements of your network.

**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.

**Best practices - Configuring the Stream Detector**

Configuring the Stream Detector, you can set up a way to handle streaming media. The recommended way is to perform a special kind of scanning when the Stream Detector has found that a web object belongs to this media type.

Virus and malware filtering on Web Gateway usually requires that web objects are completely downloaded and scanned by the Anti-Malware module (also known as engine or filter). However, as completeness can never be achieved for streaming media, the usual scanning method will not deliver results, but delay processing of this media type endlessly.

Streaming media must therefore be handled in a special way. Two components on Web Gateway are available for this:

- The Stream Detector detects that a web object is streaming media.
- The Media Stream Scanner scans streaming media chunk-by-chunk.

Compared to the usual method, the Media Stream Scanner performs a less intensive way of scanning.

Following the progress made by the Media Stream Scanner, streaming media is also delivered chunk-by-chunk to the client that a download request was received from. If an infection is detected in a chunk, the process is stopped, and this chunk and the rest of the streaming media are not delivered.

The Stream Detector is a separate module on Web Gateway, not a part of the Anti-Malware module like the Media Stream Scanner.
A suitable rule calls both components to perform their jobs. It is contained in the default Gateway Anti-Malware rule set.

However, the rule is not available in older versions of McAfee Web Gateway. So we recommend that you do the following:

- Inspect your rule set system.
- If the rule is not included in the default Gateway Anti-Malware rule set or any other rule set you are using for virus and malware filtering, configure the rule in one of these rule sets.

Make sure you place it immediately before the rule that triggers the usual anti-malware scanning.

**Rule for streaming media filtering**

The default rule for streaming media filtering looks as follows:

**Name**

**Start Media Stream Scanner on streaming media and skip anti-malware scanning**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle.Name equals &quot;Response&quot; AND</td>
<td>Stop Ruleset</td>
<td>Enable Media Stream Scanner</td>
</tr>
<tr>
<td>StreamDetector.IsMediaStream&lt;Default Streaming Detection&gt; equals true</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the default Gateway Anti-Malware rule set, this rule is placed immediately before the rule that triggers the usual anti-malware scanning.

When the Stream Detector finds that a web object is streaming media, the rule stops processing for this rule set and starts the Media Stream Scanner, so the special way of scanning streaming media is performed and the rule for the usual scanning is skipped.

The criteria part that uses the Cycle.Name property ensures that the rule only applies in the response cycle of processing when web objects are received on Web Gateway from the web, in response to a request that was forwarded.

**Settings for the Stream Detector**

The settings for the Stream Detector module can be accessed on the settings tree under Stream Detector. The name of the default settings is Default Streaming Detection.

The default settings include only the following option:

**Minimal probability** — Sets the probability of being streaming media that is sufficient for treating a web object as streaming media.

- The probability is measured in percent and configured as a number from 1 to 100.
- The probability is found by the Stream Detector. If the minimal probability is reached, the StreamDetector.IsMediaStream property, which is used in the default rule for streaming media filtering, is set to true.
- The default minimal probability is 60. We recommend that you leave this value unchanged.
Global whitelisting

Global whitelisting ensures that all further filtering is skipped for the web objects that are whitelisted, so access to them cannot be blocked.

The global whitelisting process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- Whitelists are used by rules to let some web objects skip further filtering.

A default process for global whitelisting is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure global whitelisting, you can work with:

- **Key elements of rules** — After clicking the default *Global Whitelist* rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

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**

<table>
<thead>
<tr>
<th>Criteria – Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

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 SSL scanning process includes several elements, which contribute to this in different ways.

- SSL scanning rules control the process.
- Whitelists and other lists that are used by the rules to let web objects skip SSL scanning and to perform other functions within the process.
- SSL scanning modules, which are called by the rules, perform certificate verification and other functions within the process.

To configure SSL scanning, you can work with:

- **Key elements of rules** — After clicking the default SSL Scanner rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

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.

  ![Best practice: Replace the default certificate authority that is provided for use after the initial setup with 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 certificate 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**.

**Replace the default root certificate authority**

You can replace the default root certificate authority that is provided after the initial 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 217*
  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 218*
  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.
Using AIA entries for certificate downloads

Certificates missing in a chain of server certificates that a client requires for SSL-secured communication can be downloaded using URLs that are specified in Authority Information Access (AIA) entries. AIA entries are included in the last certificate of a certificate chain.

AIA downloads are performed by the Certificate Chain module (or engine) of Web Gateway, which acts as a proxy in this communication. Only one AIA download is performed per handshake. Downloaded certificates are cached for 24 hours and re-used for other connections.

A certificate chain is considered complete once it ends in a trusted certificate authority (CA). If SSL-secured connections are tunneled, for example, due to whitelisting or for client authentication, the client must also obtain the missing certificates, which can again be achieved using URLs specified in AIA entries.

To enable AIA downloads, you must make sure that the setting for this download is selected on the user interface of Web Gateway. The setting is selected by default.

The setting is part of the Default settings for the Certificate Chain module. It can also be accessed when editing the Certificate chain filters element in the key elements view of the SSL Scanner rule set.

Sending tapped SSL traffic to a monitoring device

You can send tapped SSL traffic in decrypted format through an interface on a Web Gateway appliance to a monitoring device.

SSL-secured traffic can be tapped on Web Gateway, which means that its content is looked into. Tapping is a "silent" inspection method, as the traffic is only looked into and not interfered with otherwise.

You can configure more than one interface to send copies of the decrypted traffic to different monitoring devices.

Tapping can be applied on Web Gateway to SSL-secured traffic under HTTPS, including any subversion of this protocol. HTTP2 is, however, not supported. When tapping is configured on Web Gateway, HTTP2 traffic is not processed.

The Enable SSL Tap event is provided, which must be included in a suitable rule to enable the tapping. The rule must be applied when the CONNECT call is handled within the process of performing SSL-secured communication.

Sample rule for enabling SSL tapping

The following conditions must be met when using a rule with an event for enabling SSL tapping:

- The rule must be placed in a rule set that has Command.Name equals "CONNECT" as one of its criteria. This is the case in the embedded Handle CONNECT Call rule set of the default SSL Scanner rule set.
- The rule set must be configured for the request cycle.
- Content inspection must be activated. This is the case if you enable the embedded Content Inspection rule set of the default SSL Scanner rule set.

A suitable property for the rule criteria is, for example, Client.IP or URL.Host. A rule that enables SSL tapping for all traffic sent in requests for access to hosts that are on a particular list might look as follows.
**Configure the sending of tapped SSL traffic to a monitoring device**

Configure the sending of tapped SSL traffic to a monitoring device by configuring an interface to this device on Web Gateway and creating a rule that enables the tapping.

**Task**

1. Configure at least one interface to a monitoring device.
   a. Select Configuration | Appliances.
   b. On the appliances tree, select the appliance that you want to configure an interface on, then click SSL Tap.
   c. Configure the SSL Tap settings.

2. Create a rule that uses the Enable SSL Tap event.

3. Click Save Changes.

SSL traffic can now be tapped and sent in decrypted format to the monitoring devices that you configured interfaces for. The tapped traffic is sent if the rule that you created applies.

**SSL Scanner rule set**

The SSL Scanner rule set is the default rule set for SSL scanning.

<table>
<thead>
<tr>
<th>Default rule set – SSL Scanner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Handle CONNECT Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Command.Name equals “CONNECT”</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Certificate Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Command.Name equals &quot;CERTVERIFY*&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

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

The 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**


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.FirstKnownCAsTrusted<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 if 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.CertificateRequested 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

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)**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Connection.SSL.TransparentCNHandling equals true AND Command.Name does not equal “CONNECT” AND Command.Name does not equal “CERTVERIFY”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

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 if 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.

Hardware Security Module

Use of a Hardware Security Module (HSM) enhances security when dealing with private keys for the certificates that are exchanged between clients and servers in SSL-secured communication.

Keys for SSL-certificates can be public or private. If you are using private keys and do not want to expose them, you can store them on a Hardware Security Module.

When a key is required for enabling the use of a certificate, the key is referenced by its ID (also known as key name) while remaining protected on the module.

This method of key handling provides greater security than storing private keys in a file within your file system, as this file might be read or copied after unauthorized access to a Web Gateway appliance. The private keys on the Hardware Security Module, however, would still remain protected.

Different solutions can be implemented to provide the functions of a Hardware Security Module on Web Gateway.

Using a Hardware Security Module

Several components are involved when a Hardware Security Module is used on Web Gateway.

HSM Agent

The HSM Agent runs as a daemon within the Web Gateway appliance system. This agent enables the handling of the Hardware Security Module.

Depending on how the module is implemented, the agent addresses the module card, the remote server, or the emulation.

The agent provides a command line interface for performing activities on the module, such as generating, storing, or unlocking keys.

Module card

A module card can be installed as a hardware component on a Web Gateway appliance to provide the functions of a Hardware Security Module.

The module card that is available for use with Web Gateway is the nShield Solo HSM card. This solution is provided by an Intel partner (Thales).

When the module card is installed, you can access it by logging on to the appliance from a system console.

For more information, see the documentation of the Intel partner (Thales).
Remote server
The functions of a Hardware Security Module can be provided on a Web Gateway appliance using a remote server. The remote server that is available for use with Web Gateway is SafeNet Network HSM server. This solution is provided by an Intel partner (Gemalto).

When the remote server has been set up and connected to the appliance, you can access the module by logging on to the appliance from a system console.

For more information, see the documentation of the Intel partner (Gemalto).

Emulation
An emulation can be run on Web Gateway, which provides the functions of a Hardware Security Module using OpenSSL.

As this solution does not include a module card or remote server for storing private keys, you must store these keys manually in a directory of the appliance system.

This solution is not considered as secure as using a module card. When implemented on a standalone appliance, however, it compares to the remote server solution with regard to security. An emulation is preferably used for demos, tests, and training.

Client-server model for multiple appliances
When multiple Web Gateway appliances are part of an HSM solution, they can be configured to follow the client-server model.

This means, for example, that you need not install a module card on every Web Gateway appliance in your network to use the functions of a Hardware Security Module. Appliances that have no HSM solution of their own implemented can connect to an appliance with this solution to use its functions.

The appliance that has an HSM solution implemented then takes the server role towards the other appliances, which connect to it as clients.

On the user interface of Web Gateway, an appliance that has an HSM solution of its own implemented is referred to as HSM server even if no other appliances are configured as its clients.

The client-server model can be configured for Web Gateway appliances regardless of the particular solution (module card, remote server, or emulation) that is implemented on one of them.

Web Gateway as client of a remote server (Gemalto)
When the HSM solution on a Web Gateway appliance uses the remote server that is provided by an Intel partner (Gemalto), the client-server model also applies. The Web Gateway appliance then connects as client to the remote server.

When a Web Gateway appliance has the HSM solution implemented that uses a remote server (Gemalto) and other appliances connect to it to use the functions of this solution, this Web Gateway appliance takes both the roles of a client and a server.

The appliance then acts as a client towards the remote server (Gemato) and as a server towards the other appliances.

Key handling with a Hardware Security Module
Using a Hardware Security Module allows you to perform several activities for enhancing private key security, such as generating, storing, and referencing keys.

When an HSM solution is implemented, all cryptographic operations related to using a private key for a certificate are performed on the Hardware Security Module.
Keys can be generated on the module, but can also be imported to it. To be available on Web Gateway, they are loaded by the HSM Agent. To enable key loading, the key IDs must be made known to the agent.

Generating private keys often includes the use of passwords or an Operator Card System (OCS) to create additional security. Keys can also be generated, however, without any of these additional options.

To enhance security in key handling, responsibilities can be assigned to different administrators. For example, one administrator might be responsible for generating private keys on a Hardware Security Module.

The Web Gateway administrator then references the keys to configure certificates on the user interface of Web Gateway.

The Web Gateway administrator must know the key IDs that are generated, as well as the passwords that might be set for the keys.

Private key operations involving the Hardware Security Module are logged on Web Gateway. Information about these operations is displayed on the dashboard of the user interface.

Connection traces can also be generated for traffic on the connections between the components of a Hardware Security Module solution.

**Work with a Hardware Security Module**

Complete these high-level steps to enhance private key security with a Hardware Security Module. Different administrators can be responsible for different steps.

**Task**

1. Implement a solution for using a Hardware Security Module on a Web Gateway appliance.

   
   For information about how to generate these keys, see the following documentation:
   
   • If you installed a module card, see the documentation of the Intel partner who provides this card (Thales).

   For more enhanced security, this documentation also provides information on creating a Security World and an Operator Card Set.

   • If you have set up a remote server, see the documentation of the Intel partner who provides this server (Gemalto).

   If you use an emulation, generate private keys on the user interface of Web Gateway.


   For information on storing these keys, see the documentation of the Intel partners if you are working with a module card (Thales) or a remote server (Gemalto).

   You can also store private keys on a module card or remote server that you have generated on the user interface of Web Gateway.

   If you use an emulation, store the private keys in a directory that is provided within the Web Gateway appliance system. The path to this directory is: /opt/mwg/data/hsmagent.
4. Make private keys available for use on Web Gateway. This is done by entering them in a list on the user interface.

5. Reference private keys on a Hardware Security Module for use on Web Gateway. If you have protected the keys using an Operator Card Set, you must unlock them first. For information about how to unlock keys, see the documentation of the Intel partner who provides the Operator Card Set (Thales).

**Implement an HSM solution on an appliance**

To implement an HSM solution on a Web Gateway appliance, complete some preparatory activities. Then use the options of the user interface to select and configure a solution.

The following steps can be in the responsibility of different administrators.

**Task**

1. Prepare a Web Gateway appliance for running an HSM solution.
   - If using a module card:
     - Install the module card on the appliance.
     - For information about how to install the module card, see the *McAfee Web Gateway Installation Guide*.
   - If using a remote server:
     - Set up the remote server and connect it to the appliance.
     - For more information, see the documentation of the Intel partner who provides the remote server (Gemalto).
   - Using an emulation requires no preparatory activities.

2. On the user interface of Web Gateway, configure the HSM solution for the appliance that you have prepared.
   - Select **Configuration | Appliances**.
   - On the appliances tree, select the appliance and click **Hardware Security Module**.
     - The **Hardware Security Module** settings appear in the configuration pane.
   - Under **HSM Server**, select **Start local HSM server**.
   - From the **Crypto module** list, select one of the following HSM solutions according to what you have prepared:
     - **Thales nShield Solo** — Enables use of the module card
     - **SafeNet Network HSM (formerly Luna SA)** — Enables use of a remote server (Gemalto)
     - **OpenSSL** — Enables use of an emulation

3. In the **Keys to be loaded** list, add entries for the private keys that you want to be available for loading. For every key, enter its key ID in string format.

4. Make sure that **Allow local connections** is selected.

5. Click **Save Changes**.
You can now reference private keys when importing certificates for SSL-secured communication on the user interface of Web Gateway.

You can also configure other Web Gateway appliances that have no HSM solution of their own implemented to use the functions of the solution on this appliance.

**Enable use of the nShield Connect appliance solution**

When using an nShield Connect appliance, you must start the nShield daemon, also known as *hardserver* daemon, manually to enable this solution.

The daemon is started within the MLOS operating system of the Web Gateway appliance that you are using for the solution.

**Task**

1. Log on to the MLOS shell.
2. Run a command like the following to add a line for enabling a start script to the appropriate configuration file:
   ```bash
   echo NFP_ALWAYS_ENABLED=1 >> /etc/nfast.conf
   ```
   The `NFP_ALWAYS_ENABLED` parameter enables or disables the `/etc/init.d/nfast` script, which is used for starting the daemon.
3. Start the daemon:
   ```bash
   /etc/init.d nfast start
   ```
   Whenever the appliance system is restarted in the following, the daemon is also started.
   
   To stop the daemon, run `/etc/init.d nfast stop`.
   
   To disable the daemon permanently, set `NFP_ALWAYS_ENABLED` to zero or remove the line with this parameter from the configuration file.

**Sample procedure for configuring a remote server (Gemalto)**

Configure the remote server (Gemalto) by running suitable commands from a system console.

For information about how to configure this remote server, you should generally refer to the partner documentation (Gemalto).

The following procedure provides some sample steps and commands for completing this configuration.

**Task**

1. From a system console, connect to the remote server (Gemalto), then run the following commands to configure the server for connecting to the Web Gateway appliance.
   ```bash
   client register -c <label> -ip <IP address of the Web Gateway appliance>
   client register -c <label> -ip <IP address of the Web Gateway appliance>
   ```
2. Connect to the Web Gateway appliance, then complete these substeps.
   a. Verify the connection to the remote server.
      ```bash
      /opt/gemato/lunaclient/bin/vtl verify
      ```
   b. Create a client certificate for connecting to the remote server.
      ```bash
      /opt/gemato/lunaclient/bin/vtl createCert -n <IP address of the Web Gateway appliance>
      ```
c  Copy the client certificate to the remote server.
   scp/opt/gemato/lunaclient/cert/client/<IP address of the Web Gateway appliance>.pem admin@<domain name>

3  On the remote server, copy a server certificate to the Web Gateway appliance.
   scp admin@<domain name>:server.pem

**Configure the use of an HSM solution by multiple appliances**

Configure Web Gateway appliances that have no individual HSM solution implemented as clients of a Web Gateway appliance with an HSM solution. These appliances can then use the functions of the solution.

**Task**

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

2  On the appliances tree, select a Web Gateway appliance that has an HSM solution implemented, then click **Hardware Security Module**.

   The **Hardware Security Module** settings appear in the configuration pane.

3  Under **HSM Server**, configure this appliance to act as a server allowing clients to use a Hardware Security Module remotely.
   a  Click **Allow remote connections**.
   b  In the **HSM server port definition** list, add one or more ports that listen to client requests.
   c  Under **Server identification**, generate or import a certificate for the server. Then export it to a location where you can import it from when configuring the clients.
   d  Click **Save Changes**.

4  Complete the following substeps for every appliance that you want to configure as a client.
   a  On the appliances tree, select an appliance that has no HSM solution implemented, then click **Hardware Security Module**.
   b  Under **HSM Client**, select **Use remote HSM server**.
   c  In the **Remote server** list, add a host name with a listener port and import the server certificate.
      You can add entries for more than one server to allow this client the use of Hardware Security Modules on different servers.
   d  Under **Client identification**, generate or import a certificate for the client. Then export it to a location where you can import it from when configuring the list of appliances that are permitted as clients of the server.

5  Add the clients of the server.
   a  On the appliances tree, select the appliance that you have configured as server, then click **Hardware Security Module**.
   b  In the **Permitted clients** list under **HSM Server**, add a host name and import a certificate for every appliance that you have configured as client.

6  Click **Save Changes**.
Make private keys available on an appliance

Make private keys available for referencing in a list on a Web Gateway appliance that has an HSM solution implemented.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select an appliance that has an individual HSM solution implemented and click **Hardware Security Module**.
   
   The Hardware Security Module settings appear in the configuration pane.
3. Under **HSM Server**, add entries for private keys in the **Keys to be loaded** list.
   
   For every key, enter its key ID in string format.
4. Click **Save Changes**.

The private keys are now available for referencing.

Reference a private key on a Hardware Security Module

Reference a private key on a Hardware Security Module to make the key information available for enabling the use of a certificate.

Certificates are involved when settings for filtering SSL-secured communication are configured. This sample procedure describes one scenario for referencing a private key.

**Task**

1. Select **Policy** | **Settings**.
2. On the Engines branch of the settings tree, expand **SSL Client Context with CA** and select the **Default CA** settings.
3. Under **Define SSL Client Context**, click **Import** next to **Certificate Authority**.
   
   The Import Certificate Authority window opens.
4. Click **Browse** next to **Certificate**, then locate and import a certificate file.
5. Select **HSM** next to **Private key source**.
   
   A list with the IDs for the available private keys opens.
6. Select a key ID, then click **Import** to import the certificate with its key information.
7. Click **Save Changes**.

Advanced Threat Defense

After a web object has been scanned by Web Gateway for infections by viruses or other malware, it can additionally be scanned by the McAfee® Advanced Threat Defense (Advanced Threat Defense) web security product.

Advanced Threat Defense uses a sandboxing approach for scanning, which means that the behavior of a particular web object in a "sandbox" environment is analyzed. The scanning result is recorded in a report and delivered to Web Gateway.

The additional scanning performed by Advanced Threat Defense is also referred to as **offline scanning** or **background scanning**.
To enable the use of Advanced Threat Defense, suitable rules must be implemented on Web Gateway. You can import rule sets that contain such rules from the rule set library.

To configure the use of Advanced Threat Defense on Web Gateway, you can work with:

- **Key elements of rules** — After importing the library rule sets for the use of Advanced Threat Defense and clicking them on the rule sets tree, you can view and configure key elements of the rules for the additional scanning process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the rules for the additional scanning process completely, configure all their elements, including the key elements, and also create new rules or delete rules.
  
You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

**Options for configuring the use of Advanced Threat Defense**

You can configure different options to implement an additional scanning by Advanced Threat Defense.

- **Forwarding a web object depending on the additional scanning** — When this option is configured, the result of the additional scanning by Advanced Threat Defense determines whether a web object is forwarded to the user who requested it.
  
If a web object is found to be safe, it is forwarded, otherwise not.

- **Forwarding a web object before the additional scanning** — When this option is configured, a web object is forwarded to the user who requested it, before the additional scanning by Advanced Threat Defense.
  
If a web object is found to be infected, a warning message is sent to the administrator of the network that the user sent his request from.

You can also configure that a web object is not scanned a second time by Advanced Threat Defense if it has been scanned before. In this case, the existing report that was produced after the first scanning is evaluated once again.

**Availability of Advanced Threat Defense**

For use with Web Gateway, the Advanced Threat Defense web security software is delivered pre-installed on the same hardware platform, where it runs as an appliance on a separate server.

Several instances of the product can also run on different servers and be used to support Web Gateway. Each instance of the product must be installed on its own hardware platform.
Workflows for using Advanced Threat Defense

Different workflows can be configured when Advanced Threat Defense is used to perform an additional scanning of web objects.

Forwarding a web object depending on the additional scanning

The following diagram shows the workflow that forwards a web object to a user depending on the scanning result of Advanced Threat Defense.

Figure 10-1  Web object is forwarded depending on additional scanning result

1. A user sends a request to access a web object, for example, a file, from a system within your network that is a client of Web Gateway.

2. If the request passes filtering according to the configured rules, Web Gateway forwards it to the appropriate web server.
   
   A progress page is sent to the client, telling the user to wait while the request is processed.

3. The web server sends the object to Web Gateway.

4. If the criteria for using Advanced Threat Defense are met, Web Gateway passes the object on for scanning.

   To retrieve information on the scanning progress, Web Gateway queries Advanced Threat Defense in regular intervals.

5. When Advanced Threat Defense has completed the scanning, it lets Web Gateway know whether the object is malicious or not.

6. Depending on this information, Web Gateway allows the user to access the requested object or sends a block page, which states that access is blocked and gives a reason for the blocking.
Criteria for additional scanning by Advanced Threat Defense

Web Gateway uses the functions of Advanced Threat Defense for scanning a web object after the object has been scanned by the anti-malware engines on Web Gateway.

The Advanced Threat Defense library rule set uses this probability in its criteria. The default value that must be reached for the criteria to match is 60. This means that only if scanning a web object on Web Gateway results in a malware probability of 60 percent or more, is it passed on to Advanced Threat Defense.

When configuring the use of Advanced Threat Defense, you can increase or lower this value and, consequently, let this product support Web Gateway more or less frequently.

It is therefore important that, on the rule sets tree, the rule set for Advanced Threat Defense is placed behind the rule set for the normal anti-malware functions on Web Gateway, which is usually the Gateway Anti-Malware default rule set.

The Anti-Malware module (or engine) runs with two different settings, when Web Gateway and Advanced Threat Defense work together: one for the Web Gateway part and one for the part of the supporting product.

The default names of the two settings are Gateway Anti-Malware and Gateway ATD.

One important point in which the settings differ from each other is that the Gateway ATD settings have the option for using Advanced Threat Defense selected, whereas this option is deselected in the other settings.

Configuration elements for using Advanced Threat Defense

To enable the additional scanning of web objects by Advanced Threat Defense, suitable rules must be implemented on Web Gateway. You can import rule sets that contain such rules from the rule set library. After importing this rule set, a list and settings are also implemented.

Rule sets for the additional scanning

There is a rule set for forwarding a web object depending on the additional scanning, as well as a rule set for forwarding a web object before the additional scanning and delivering any warning information afterwards.

• Advanced Threat Defense library rule set — This rule set implements the workflow that lets a web object additionally be scanned by Advanced Threat Defense and forwarded to the user depending on the scanning result.

After importing this rule set, a list and settings are also implemented.
• **ATD - Init Offline Scan nested library rule set** — This nested rule set has the same criteria as the rule set that forwards a web object to the user depending on the result of the additional scanning.

The rule set applies if previous scanning by Web Gateway has resulted in a configured degree of probability that a web object is infected, the web object is on the list of web objects that can be scanned, and a particular object size is not exceeded.

The rule set contains only one rule that uses the `Antimalware.MATD.InitBackgroundScan` property in its criteria. The value of this property is `true` by default.

In this case, data for the current transaction is recorded. This includes all data that is related to a request for web access and the response to it from a web server, such as the IP address of the client, authentication information, the URL of the web server, and the requested web object that was sent as the body of the response message.

An internal request is sent to initiate scanning by Advanced Threat Defense. After this has been completed, the requested web object is forwarded to the user while the scanning is performed later on, using the data that was recorded.

If the value of the `Antimalware.MATD.InitBackgroundScan` property is `false`, scanning by Advanced Threat Defense could not be initiated and a rule event is used to display an error message.

• **ATD - Handle Offline Scan nested library rule set** — This nested rule set has the `Antimalware.MATD.IsBackgroundScan` property for its criteria. The value of this criteria is `true` by default.

In this case, the data that was recorded by the rule in the `ATD - Init Offline Scan` rule set, is used by Advanced Threat Defense to scan the web object specified by the data.

The rule set has a rule that uses an event to increase a counter if a scanned web object has been found to be infected, a rule that uses another event to create and send a message about the infected web object to the administrator, and finally a rule that stops the processing cycle.

### List and settings for the additional scanning

The Advanced Threat Defense library rule set provides rules for enabling the use of Advanced Threat Defense on Web Gateway and forwarding a requested web object to the user depending on the scanning result.

After importing this rule set, a list and settings are also implemented.

• **Advanced Threat Defense Supported Types list** — This list is used within the criteria of the library rule set. Only web objects belonging to the media types on this list are passed on to Advanced Threat Defense for scanning.

The list contains several media types by default. You can add media types to the list or remove them.

• **Gateway ATD settings** — These are settings for the Anti-Malware module (or engine) on Web Gateway, which handles virus and malware filtering, including the additional use of Advanced Threat Defense.
The settings include mainly options for configuring the following:

- Communication between Web Gateway and the server that Advanced Threat Defense runs on
- Severity grade that lets a web object, for example, a file, be classified as malicious

When an object is scanned by Advanced Threat Defense, the result is a severity grade on a scale from 0 to 5 (very high severity).

You can set a value on this scale, for example, 3, which means all objects with a scanning result of 3 or higher are considered to be malicious.

For these objects, the Antimalware.Infected property is set to true, so a rule that uses this property in its criteria will block a web object and prevent it from being passed on to the user who requested access to it.

**Using an existing Advanced Threat Defense scanning report**

A report that is generated by Advanced Threat Defense after scanning a web object can be used by Web Gateway to evaluate this object and handle access to it.

When using an existing report, Web Gateway will not trigger a new scanning run on Advanced Threat Defense. If more than one report exists, the latest report is used for evaluation. Hash values are calculated internally on Web Gateway to determine whether a web object is the same as another object, so the same report can be used.

To use an existing scanning report on Web Gateway, you need to implement a rule with the Antimalware.ATD.GetReport property. If the value of this Boolean property is true, it means that a particular web object has been found to have already been scanned by Advanced Threat Defense and a report for this scan has been retrieved.

This report can be made available to other rules, for example, to a rule with the Antimalware.Infected property, which evaluates the report to find out whether an object is infected.

**Options for using an existing scanning report**

There are several options for using an existing scanning report to handle access to web objects.

- **Allow a file when a scanning report shows that it is not infected** — There are files that are uploaded manually to Advanced Threat Defense where they are scanned and a report is generated. Web Gateway then allows users to download such a file if a report exists for it and this report shows that the file is not infected.

If a scanning report does not exist for a web object, the Antimalware.ATD.GetReport property can still be used in suitable rules. In these rules, the value of this property is false, as no scanning report was retrieved.

- **Allow a file if no scanning report is available and scan this file offline** — If no scanning report exists for a file that was requested for downloading, a rule can allow a user to download the file and let an offline scan be performed. After the scanning, a report is generated and forwarded to the administrator of the user’s network.

- **Block a file if no scanning report is available and scan this file offline** — If no scanning report exists for a file that was requested for downloading, a rule can block access to the file and let an offline scan be performed. After the scanning, a report is generated and forwarded to the administrator of the user’s network.

**Sample rules for using an existing scanning report**

There is no preconfigured rule set for using an existing Advanced Threat Defense scanning report in the default rule set system or the rule set library. You can, however, create suitable rules and a rule set for them on your own.
The following sample rules implement the solution that lets files be uploaded manually to Advanced Threat Defense. Downloading a file is allowed if the report that was generated by Advanced Threat Defense shows that the file is not infected.

The name of the rule set might be Use Existing Advanced Threat Defense Scanning Report. It must have the same criteria regarding media types as the Advanced Threat Defense library rule set and apply for all processing cycles.

The rule set should contain the following rules:

- A rule that uses the 
  \texttt{Antimalware.ATD.GetReport} property to retrieve an existing scanning report

- A rule that evaluates files using this report and blocks access if the report shows that they are infected

The rule that retrieves the report might look as follows:

\begin{verbatim}
Name Allow files that have been scanned before
Criteria \texttt{Antimalware.ATD.GetReport equals false} -> Block <BlockedByMATD>
Action - Statistics.Counter.Increment" (BlockedByMATD",1)<Default>
\end{verbatim}

The rule blocks access to a file if no report exists for it. In this case, the next rule is not processed. This rule evaluates a report. It might look as follows:

\begin{verbatim}
Name Block infected files
Criteria \texttt{Antimalware.Infected <Gateway ATD> equals true} -> Block <BlockedByMATD>
Action - Statistics.Counter.Increment ("BlockedByMATD",1)<Default>
\end{verbatim}

In both rules, a counter records how often files were blocked when Advanced Threat Defense functions were used.

**Using an ongoing Advanced Threat Defense scanning run**

While a scanning run is being performed by Advanced Threat Defense, the results of this run can be used not only for processing the request that it was started for, but also for other requests to access the same web object.

To let the results of one scanning run be used for processing multiple requests, the requests must be received on Web Gateway while the scanning is still going on. Hash values are calculated internally on Web Gateway to determine whether a web object is the same as another object, so it can be decided whether requests for the same object are received.

To use the results of one scanning run for multiple requests to access the same object, you need to enable an option within the Gateway ATD settings for the Anti-Malware module (or engine), must be enabled. The name of this option is Re-use running task if same sample is being analyzed.

There is no preconfigured rule set in the default rule set system or the rule set library for using the results of one scanning run when multiple requests for the same object are received. You can, however, create suitable rules and a rule set for them on your own.
Limiting object sizes for scanning by Advanced Threat Defense

The size of objects that are additionally scanned by Advanced Threat Defense must be checked for compliance with the size limits that exist for this product.

There are some restrictions for Advanced Threat Defense regarding the size of web objects that can be scanned. The general size limit is 125 MB, which means that web objects of any type must not exceed this limit.

Other size limits exist for particular types of web objects. This is mainly due to the fact that sandboxing is performed on Advanced Threat Defense, which only allows, for example, a size of 10 MB for executable files.

Impact on the user experience

Web Gateway and Advanced Threat Defense communicate with each other over a REST API, which accepts files up to the general size limit by default. An end user who sent, for example, a request for downloading a 30 MB file is therefore first led to believe that this size is allowed.

When the sandboxing functions start operating, however, the file is rejected as too large. The end user receives a block message from Web Gateway, and the Advanced Threat Defense administrator sees an error message.

Configuring size limits on Advanced Threat Defense

File size limits can be set on Advanced Threat Defense using the `set filesizes` command.

Best Practice: Set all file size limits on Advanced Threat Defense to the same value.

We also recommend implementing this value on Web Gateway, for example, by creating a rule that only forwards files for scanning to Advanced Threat Defense if they do not exceed the size limit.

For more information about default size limits on Advanced Threat Defense and the methods of changing them, see the *McAfee Advanced Threat Defense Product Guide*.

Configuring size limits on Web Gateway

On Web Gateway, you can configure a rule that blocks files if they exceed a particular size limit. By inserting this rule in a rule set for handling Advanced Threat Defense scanning activities, you can make sure that only files with suitable sizes are passed on to Advanced Threat Defense.

If you have imported the library rule sets for Advanced Threat Defense, you can insert the size limiting rule there. Some of these rule sets contain a rule for uploading web objects to Advanced Threat Defense.

By inserting the size limiting rule before this rule, files that exceed the size limit are blocked and the rule for uploading to Advanced Threat Defense is not executed.

Rule for setting a size limit

The following sample rule assumes that files must not exceed a size limit of 10 MB if they are to be scanned by Advanced Threat Defense. It blocks files that exceed this limit.

Name

Limit file size for scanning by Advanced Threat Defense

Criteria

Body.Size greater than 10000000

Action

Block<ATD size limit>

To let the size check only apply to particular file types, suitable parts must be added to the rule criteria. For example, if you only want to cover executable files, you can add a criteria part that uses the `MediaType.IsExecutable` property.
To let the user who sent a request involving an over-sized object to the web know that and why this request was blocked, you can configure appropriate settings for the block action. In the sample rule, these settings are named ATD size limit.

**Configure the use of Advanced Threat Defense**

You can configure the use of Advanced Threat Defense for additionally scanning web objects after they have been scanned by Web Gateway. Another option is to let a scanning report that has been generated for a web object by Advanced Threat Defense be evaluated on Web Gateway to handle access to this object.

If an existing scanning report for a web object is evaluated, Web Gateway will not trigger a new additional scanning run by Advanced Threat Defense for this object.

**Tasks**

- **Configure scanning by Advanced Threat Defense on page 240**
  Configure additional scanning by Advanced Threat Defense after a scanning run by Web Gateway has been completed.

- **Configure use of an existing Advanced Threat Defense scanning report on page 241**
  If you do not want a new scanning run to be performed on a web object, you can let an existing Advanced Threat Defense scanning report be used to evaluate the web object.

**Configure scanning by Advanced Threat Defense**

Configure additional scanning by Advanced Threat Defense after a scanning run by Web Gateway has been completed.

**Task**

1. Configure Advanced Threat Defense to integrate it into your network.
   For more information, see the McAfee Advanced Threat Defense Product Guide.

2. On the user interface of Web Gateway, complete the following activities:
   a. Import the rule set for one of the two additional scanning workflows from the rule set library.
      These rule sets are located in the Gateway Anti-Malware rule set group.
      
         • **Advanced Threat Defense** — For forwarding web objects depending on the additional scanning
           On the rule sets tree, place this rule set after the rule set for scanning by Web Gateway. By default, this is the Gateway Anti-Malware rule set.

         • **ATD - Offline Scanning with Immediate File Availability** — For forwarding web objects before the additional scanning
           After importing this rule set, the following two rule sets appear on the rule sets tree.

           • **ATD - Init Offline Scan** — This rule set that initiates the additional scanning.
             On the rule sets tree, place this rule set after the rule set for scanning by Web Gateway. By default, this is the Gateway Anti-Malware rule set.

           • **ATD - Handle Offline Scan** This rule set handles the additional scanning once it has been initiated.
             On the rule sets tree, place this rule set after the rule sets that perform global or common activities and before the rule sets that perform particular filtering activities.

             For example, on the default rule sets tree, place this rule set after the Common Rules rule set and before the Media Type Filtering rule set.
To enable monitoring of Advanced Threat Defense scanning activities on Web Gateway, import the **ATD Scanning Log** and **Block on ATD Errors** rule sets from the rule set library and add them to the existing Log Handler and Error Handler rule sets, respectively.

Add media types to the list for supported media types or remove them as needed. After importing either of the library rule sets, the name of this list is **Advanced Threat Defense Supported Types**.

Configure the settings for scanning by Web Gateway. By default, the name of these settings is **Gateway Anti-Malware**.

Configure the settings for scanning by Advanced Threat Defense. After importing either of the library rule sets, the name of these settings is **Gateway ATD**.

Save your changes.

**Configure use of an existing Advanced Threat Defense scanning report**

If you do not want a new scanning run to be performed on a web object, you can let an existing Advanced Threat Defense scanning report be used to evaluate the web object.

There are several options for using an existing scanning report. The following task assumes that:

- Scanning reports were generated for web objects that were uploaded manually to Advanced Threat Defense and scanned.

- Web Gateway allows access if a report shows that a web object is not infected and blocks it if no report exists.

Complete the following high-level steps:

**Task**

1. Create a rule set for the rules that handle the use of an existing Advanced Threat Defense scanning report.

2. In this rule set, create the following.
   - A rule that retrieves a scanning report for a file and blocks access to a file if no report exists for it
   - A rule that evaluates a scanning report and blocks a file that is infected according to the report

3. Configure the **Gateway ATD** settings of the Anti-Malware module.
   a. Make sure **Re-use previous detection** is selected.
   b. [Optional] Under **Maximum detection age**, modify the time limit for excluding older reports as needed. This limit is 30 minutes by default.

4. Save your changes.
Configure key elements for using Advanced Threat Defense

Configure key elements for additional scanning by Advanced Threat Defense to adapt important parts of the scanning process to the requirements of your web security policy.

**Task**

1. Import the Advanced Threat Defense or the **ATD - Offline Scanning with Immediate File Availability** rule set from the rule set library.

2. On the rule sets tree, select the rule set that you have imported.
   - Key elements of the rules for the scanning process appear in the configuration pane.

3. Configure the key elements as needed.

4. Click Save Changes.

Configure settings for using Advanced Threat Defense

You can configure settings for the Anti-Malware module (or engine) on Web Gateway to enable the use of Advanced Threat Defense for scanning web objects.

**Task**

1. Select Policy | Settings.

2. On the **Engines** branch of the settings tree, expand **Anti-Malware** and select the settings for configuring the use of Advanced Threat Defense.
   - After importing the Advanced Threat Defense library rule set, the name of these settings is **Gateway ATD**.

3. Configure these settings as needed.

4. Click Save Changes.

Monitoring the use of Advanced Threat Defense

Several methods are available for monitoring the scanning activities that are performed by Advanced Threat Defense when it is used to support Web Gateway.

The monitoring can be done on Web Gateway and on McAfee Content Security Reporter.

**Monitoring the use of Advanced Threat Defense on Web Gateway**

On Web Gateway, you can implement rule sets with rules for logging information about the scanning jobs that Advanced Threat Defense performs and for handling errors that occur during these jobs.

You can also review Advanced Threat Defense activities on the dashboard of the user interface.

- **Log Handler** — The **ATD Scanning Log** rule set can be imported from the **Logging** group of rule sets in the rule set library.

  The rule set contains a logging rule that records information about each scanning job Advanced Threat Defense performs on a web object that was passed on to it by Web Gateway.

  This information includes:

  - Severity grade that is the result of scanning
  - Server that Advanced Threat Defense runs on
• Task ID for a scanning job
• Hash value for a scanning job

To create the log entries that provide this information, the rule uses suitable properties.

• **Error Handler** — The *Block on ATD Errors* rule set can be imported from the Error Handling group of rule sets in the rule set library.

It contains blocking rules for handling errors that occur when Advanced Threat Defense performs a scanning job.

The rules use the appropriate error IDs in their criteria. The error IDs range from 14010 to 14012.

A rule in the *Block on Anti-Malware Engine Errors* rule set covers the range from 14002 to 14050. The *Block on ATD Errors* rule set should, therefore, be placed before this anti-malware rule set.

Otherwise, the blocking rules in the *Block on ATD Errors* rule set would never be processed and only block messages with text that is related to anti-malware errors in general would be sent to users.

• **Anti-Malware properties** — Several properties are available for monitoring the activities of Advanced Threat Defense. Their names begin with `Antimalware.MATD.`, for example, `Antimalware.MATD.Server` or `Antimalware.MATD.Report`.

These properties are used in the logging rules of the ATD Scanning Log rule set.

When a scanning job has been performed by Advanced Threat Defense, the value of the `Antimalware.MATD.Report` property is a report on this job. The report is provided as a string that represents the data structure of a JavaScript Object Notation (JSON) object.

Using JSON properties together with the `Antimalware.MATD.Report` property, you can extract report information.

• **Dashboard** — The dashboard charts and tables show how the following data evolved during a particular time interval.
  
  • Under **Executive Summary**: Number of requests for web objects that were blocked due to the scanning results found by Advanced Threat Defense.
  
  • Under **Malware Statistics**: Number of requests for web objects that were passed on to Advanced Threat Defense for scanning, number of requests that were blocked due to the scanning results, and the time consumed for the scanning.

**Monitoring the use of Advanced Threat Defense on Content Security Reporter**

With McAfee® Content Security Reporter, you can collect data about the scanning activities that Advanced Threat Defense performs when it is used to support Web Gateway.

• To collect the data, configure both Web Gateway and Advanced Threat Defense as log sources.

• To view the data, register the server that Advanced Threat Defense runs on. You can then view the data on the dashboard monitor.

For more information, see the *McAfee Content Security Reporter Product Guide*. 
McAfee Advanced Threat Defense rule set

The McAfee Advanced Threat Defense rule set is a library rule set for enabling Web Gateway to work with Advanced Threat Defense when filtering web objects.

<table>
<thead>
<tr>
<th>Library rule set – McAfee Advanced Threat Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Antimalware.Proactive.Probability&lt;Gateway Anti-Malware&gt; greater than or equals 60 AND MediaType.EnsuredTypes at least one in list Advanced Threat Defense Supported Types</td>
</tr>
<tr>
<td>Cycles – Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies if the following is true:

- As a result of previous scanning by the anti-malware engines on Web Gateway, the probability that a web object is malicious equals or exceeds 60 percent
- The media type of the object is on the list of supported types for scanning by Advanced Threat Defense.

The rule set contains the following rules.

Enable progress page

Always -> Continue – Enable Progress Page<Default>

The rule enables an event that lets a page be shown to indicate the progress made when a web object is downloaded to a client.

Only send media types with high probability to MATD

MediaType.EnsuredTypes at least one in list McAfee Advanced Threat Defense Exception Types AND Antimalware.Proactive.Probability<Gateway Anti-Malware> less than 70 –> Stop Rule Set

The rule has two criteria parts, which serve to restrict the range of web objects that are passed on to Advanced Threat Defense for additional scanning.

On the one hand, the MediaType.EnsuredTypes property is used in the first part of the criteria to check whether the object that is being processed belongs to a media type that is in a particular list. This list is a McAfee-supplied list.

On the other hand, the Antimalware.Proactive.Probability property is used to find out whether the probability that the object is malicious remains below a particular value.

If both parts of the criteria match, which means the object belongs to a media type in the list and its malware probability is below the configured value, the rule applies.

Further processing of the rule set is then stopped and the rule that follows in the rule set is not processed anymore, so the object is not passed on to Advanced Threat Defense.

Upload file to ATD and wait for scanning result


The rule uses the Antimalware.Infected property to check whether a web object, for example, a file, is infected by a virus or other malware.

The scanning that is required for this check is performed under the Gateway ATD settings, which means it is carried out by Advanced Threat Defense.

If the object is found to be infected, the process of forwarding the object to the requesting client is blocked and a block message is shown to the user who requested access to the object.

The block action is recorded by the statistics counter.
ATD - Offline Scanning with Immediate File Availability rule set

The ATD – Offline Scanning with Immediate File Availability rule set is a library rule set for enabling Web Gateway to work with Advanced Threat Defense when filtering web objects.

When this rule set is implemented, a web object is forwarded to the user who requested it before it has been additionally scanned by Advanced Threat Defense, so the object is immediately available to the user.

If the scanning result is that the web object is infected, a message is sent to the administrator of the network that the user sent the request from.

This use of the scanning functions of Advanced Threat Defense is also known as offline scanning or background scanning.

After importing this rule set, the following two rule sets are implemented and appear on the rule sets tree:

- ATD - Init Offline Scan
- ATD - Handle Offline Scan

A rule set with the name ATD - Offline Scanning with Immediate File Availability is not implemented.

ATD - Init Offline Scan

This rule set initiates the additional scanning by Advanced Threat Defense.

### Library rule set – ATD - Init Offline Scan

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Antimalware.Proactive.Probability&lt;Gateway Anti-Malware&gt; greater than or equals 60 AND MediaType.EnsuredTypes at least one in list Advanced Threat Defense Supported Types AND Body.Size less than 3000000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies if the following is true:

- As a result of previous scanning by Web Gateway, the probability that a web object is malicious equals or exceeds 60 percent.
- The media type of the object is on the list of supported types for scanning by Advanced Threat Defense.
- The web object does not exceed a particular size.

The rule set contains the following rule.

**Offline scanning with immediate file availability**

*Antimalware.MATD.InitBackgroundScan(5) equals false* -> Block<ATD Communication Failed>*

When this rule is processed, all data related to the request for web access that has been sent to Web Gateway is recorded, including the response that was received from the requested web server. The response usually includes in its body the requested web object, for example, a file. The body with the web object is stored on Web Gateway.

An internal request is also created within Web Gateway to initiate the scanning by Advanced Threat Defense. Web Gateway then waits for an answer to this internal request to see whether the request is accepted and the scanning will be performed.

The time that Web Gateway waits for this answer is measured in seconds and a parameter of the *Antimalware.MATD.InitBackgroundScan* property. By default, this time is 5 seconds. You can configure this time by editing the property parameter.
If no answer to the internal request is received within the configured time, the property is set to false, so this criteria matches and the rule applies. A message is then sent to inform the administrator that the additional scanning by Advanced Threat Defense could not be executed.

If the answer is received within the configured time, the web object is forwarded to the user.

Further handling of the additional scanning is performed by the next rule set.

### Library rule set - ATD - Handle Offline Scan

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Antimalware.MATD.IsBackgroundScan equals true</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests, Embedded Objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies if the value of the `Antimalware.MATD.IsBackgroundScan` is true.

It is true if the additional scanning by Advanced Threat Defense has successfully been initiated by the rule in the preceding rule set. In this case, the data that was recorded and stored by this rule is used by Advanced Threat Defense to scan a requested web object.

The rule set contains the following rules.

#### Upload file to ATD and wait for scanning result

`Antimalware.Infected<Gateway ATD> equals true` → Continue → `Statistics.Counter.Increment("BlockedByMATD", 1)`<Default>

The rule uses the `Antimalware.Infected` property to check whether a web object, for example, a file, is infected by a virus or other malware. The scanning that is required for this check is performed under the Gateway ATD settings, which means it is carried out by Advanced Threat Defense.

For this purpose, the previously stored web object is forwarded from Web Gateway to Advanced Threat Defense.

If the scanning result is that the web object is infected, this is recorded by a statistics counter.

#### Offline scanning with immediate file availability


When the rule is processed, it is checked whether the value of the `Antimalware.Infected` property is true.

If it is, it means the scanning that was performed by Advanced Threat Defense has found a web object to be infected by a virus or other malware.

A warning message is then created and sent to the administrator for the network of the user who sent the request to access the web object. The message contains information on the request that was recorded by the rule of the preceding rule set.

#### Stop cycle

`Always` → Stop Cycle

This rule stops the processing cycle. It is always executed after the preceding rules have been processed.
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: DLP.Classification.BodyText.Matched<SOX> equals true
Action: 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 use 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 $DLP\textunderscore Classification.BodyText.Matched$ property that was already shown in a sample rule.

For the second, you can use the $DLP\textunderscore Classification.AnyText.Matched$ 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 $DLP\textunderscore Dictionaries.BodyText.Matched$ and, $DLP\textunderscore Dictionaries.AnyText.Matched$ 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 $DLP\textunderscore Classification.BodyText.Matched$ is true for the body text of a request or response that was processed, the following applies for the relevant logging properties:

- $DLP\textunderscore Classification.BodyText.MatchedTerms$ contains a list of the matching terms from the body text
- $DLP\textunderscore Classification.BodyText.MatchedClassifications$ contains a list of the matching classifications

When the value of $DLP\textunderscore Dictionary.BodyText.Matched$ is true, $DLP\textunderscore Dictionary.BodyText.MatchedTerms$ 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 $DLP\textunderscore Classification.AnyText.Matched$ is true:

- $DLP\textunderscore Classification.AnyText.MatchedTerms$ contains a list of matching terms found in text other than body text.
- $DLP\textunderscore Classification.AnyText.MatchedClassifications$ contains a list of matching classifications found in text other than body text.

When the match is in a dictionary, $DLP\textunderscore Dictionary.AnyText.Matched$ is true and $DLP\textunderscore Dictionary.AnyText.MatchedTerms$ 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**

  *DLP.Classification.BodyText.Matched<HIPAA> equals true AND*
  
  *DLP.Dictionary.BodyText.Matched<Doctors'Names> equals true*

  **Action**

  Block<DLP.Classification.Block>

**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 252**
  For data loss prevention that uses dictionary entries, you must create settings that include a dictionary.

- **Fill the dictionary with entries on page 252**
  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 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.

<table>
<thead>
<tr>
<th>Default rule set – Data Loss Prevention (DLP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – DLP in Request Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Cycle.TopName equals &quot;Request&quot;</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM) and embedded objects</td>
</tr>
</tbody>
</table>

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**

\[
\text{DLPClassification.BodyText.Matched } \langle \text{HIPAA} \rangle \text{ equals true } \rightarrow \text{Block}\langle \text{DLP.Classification.Block} \rangle \text{ – Statistics.Counter.Increment ("BlockedByDLPMatch",1)<Default>}
\]

The rule uses the `DLPClassification.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**

\[
\text{DLPClassification.BodyText.Matched } \langle \text{Payment Card Industry} \rangle \text{ equals true } \rightarrow \text{Block}\langle \text{DLP.Classification.Block} \rangle \text{ – Statistics.Counter.Increment ("BlockedByDLPMatch",1)<Default>}
\]

The rule uses the `DLPClassification.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

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 Sarbanes-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.

<table>
<thead>
<tr>
<th>Nested library rule set – DLP Response Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria ↔ <code>Cycle.TopName equals &quot;Response&quot;</code></td>
</tr>
<tr>
<td>Cycles ↔ Responses and embedded objects</td>
</tr>
</tbody>
</table>

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

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 inappropriate 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**.

**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.

<table>
<thead>
<tr>
<th>Library rule set – Data Loss Prevention With ICAP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – <strong>Criteria</strong> — <strong>URL.Host does not equal &quot; &quot;</strong></td>
</tr>
<tr>
<td><strong>Cycles</strong> – Requests (and IM) and embedded objects</td>
</tr>
</tbody>
</table>

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.IsNullOrEmpty(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.IsNullOrEmpty` 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 52428800` -> 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.

In the rule set criteria, the size of a request body that must not be exceeded is specified in bytes.

**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.

Using an on-premise DLP server from the cloud

You can perform DLP filtering using an on-premise DLP server with an ICAP client that runs in the cloud. You can only implement this method of DLP filtering if you are using the hybrid solution for Web Protection, which includes both Web Gateway and Web Gateway Cloud Service (WGCS).

The ICAP client is made available by importing a rule set on Web Gateway, which is also configured for cloud use.

The DLP server takes the role of the ICAP server in this type of configuration. The server must be placed in a DMZ where it can have a public IP address, as the ICAP client connects to it using that type of address. Internal and other protected addresses must not be used in the cloud and are therefore excluded by a check that the ICAP client performs.

ICAP client and server also send health check messages to each other in regular intervals.

We recommend using ICAPS (Secure ICAP), as data is transferred in plain text format when normal ICAP is used. The ICAP client does, however, not validate the certificate that the DLP server sends in its role as ICAP server.

ICAP-related properties for cloud use

The following properties can be used in rules for the filtering process on WGCS.

• Properties for the ReqMod mode:
  • ICAP.ReqMod.Satisfaction
  • ICAP.ReqMod.ResponseHeader.Exists
  • ICAP.ReqMod.ResponseHeader.ExistsMatching
  • ICAP.ReqMod.ResponseHeader.Get
  • ICAP.ReqMod.ResponseHeader.GetMatching
  • ICAP.ReqMod.ResponseHeader.GetMultiple
  • ICAP.ReqMod.ResponseHeader.GetMultipleMatching

• Properties for the RespMod mode:
  • ICAP.RespMod.ResponseHeader.Exists
  • ICAP.RespMod.ResponseHeader.ExistsMatching
  • ICAP.RespMod.ResponseHeader.Get
  • ICAP.RespMod.ResponseHeader.GetMatching
  • ICAP.RespMod.ResponseHeader.GetMultiple
  • ICAP.RespMod.ResponseHeader.GetMultipleMatching
Configure the use of an on-premise DLP server from the cloud

To configure the use of an on-premise DLP server from the cloud, complete the following procedure.

**Task**

1. Configure the network components that run in this solution with Web Gateway.
   a. Place the DLP server in a Demilitarized Zone (DMZ), so that it can have a public IP address.
      The ICAP client in the cloud must be able to connect to the DLP server in its role as ICAP server using the public IP address of this server.
   b. Configure the firewall to accept requests from Web Gateway Cloud Service (WGCS) on a dedicated port, which must be the ICAP server port that is also configured on the ICAP client.
      Use port 1344 when working with ICAP and port 11344 when working with ICAPS.

2. On Web Gateway, import the Data Loss Prevention (DLP) with ICAP for Cloud rule set from the library.
   - The rule set is by default configured for use in the cloud.

3. Review the Reqmod for Cloud settings, which are imported with the rule set.
Web filtering
Using an on-premise DLP server from the cloud
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 XMPP, which is the protocol used for several instant messaging services such as Jabber, Google Talk, Facebook Chat, and others.

You can also control administrator access to an appliance by setting up and maintaining administrator accounts and roles.

**Contents**

- Authenticating users
- Configure authentication
- Configure the Authentication module
- Implement a different authentication method
- Using system settings to configure authentication
- NTLM Agent authentication
- LDAP digest authentication
- Best practices - Configuring authentication for deployment types
- Best practices - Configuring LDAP authentication
- Instant messaging authentication
- One-time passwords
- Client Certificate authentication
- Administrator accounts
Authenticating users

Authenticating the users of your network ensures that they cannot access the web if they are not successfully authenticated. 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 process includes several elements, which contribute to it in different ways.

• Authentication rules control the process.
• The Authentication module, which is called by the rules, retrieves information about users from a database.

An authentication process is not implemented by default on Web Gateway after the initial setup. You can implement a process by importing suitable rule sets from the rule set library and modify this process to adapt it to the requirements of your web security policy.

To configure authentication, you can work with:

• **Key elements of rules** — After importing the library rule sets for authentication and clicking them on the rule sets tree, you can view and configure key elements of the rules for the authentication process.

• **Complete rules** — After clicking Unlock View in the key elements view, you can view the rules for the authentication process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

Authentication rules

Authentication rules usually include a rule that asks an unauthenticated user to authenticate and blocks requests from users who cannot be successfully authenticated.

There can also be whitelisting rules that allow users who send a request to skip authentication, for example, depending on the IP address that a request was sent from or the URL that is requested.

Rule sets with rules for several types of authentication, for example, IM and cookie authentication, are available in the rule sets library.

Authentication module

The Authentication module is also known as Authentication engine. It 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
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**

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 controls 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.

### 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.
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 Membership.
   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.

NTLM Agent authentication

NTLM Agent authentication uses a separate software product, known as the NTLM Agent, for authenticating users on Web Gateway.

This authentication method is an option, for example, when the connection between Web Gateway and the domain controller that is involved in the authentication process is blocked by a firewall. The NTLM Agent only requires a single freely definable port to be opened for connecting to the domain controller.

Configuring settings for the NTLM Agent

The NTLM Agent is installed on one or several Windows systems in your network. On these systems, it runs as a service that performs its authentication tasks in the background.

This service can, however, not be accessed at the system desktop. After the NTLM Agent has been installed on a system, it is therefore available as an application, which can be accessed in a directory of that system. This directory is usually the program files directory.

When the application is accessed, it opens a configuration window at the system desktop, which allows you to configure settings for the NTLM Agent.

The NTML Agent service and its application communicate with each other, so the configuration settings that you implement using the application are applied to the service.

In addition to configuring settings using the configuration window of the NTML Agent, you must also configure NTLM Agent settings on the user interface of Web Gateway.
Configure NTLM Agent authentication

Configure NTLM Agent authentication both in the user interface of Web Gateway and the configuration window of the NTLM Agent.

Task

1. Download and install the NTLM Agent software.
   b. Navigate to Products | McAfee Web Gateway 6 | Downloads | Tools.
   c. In the NTLM Agent section, click the .exe icon.
   d. Follow the instructions of the installation program.

2. Configure the settings that are provided by the NTLM Agent.
   a. After the NTLM Agent software has been installed on a system in your network, navigate to the NTLMAgent.exe file in the directory where the software was installed. The path to this file might be, for example, C:\Program Files\Secure Computing\NTLMAgent.
   b. Click the .exe file. A menu with basic options for working with the NTLM Agent opens.
   c. Click Configure. The NTLM Agent configuration window opens.
   d. Use the NTLM Agent window to configure the NTLM Agent settings.

3. Configure the settings that are provided on the user interface of Web Gateway.
   a. Select Policy | Settings.
   b. On the settings tree, expand Authentication and click one of the settings, for example, the User Database settings. The settings appear in the configuration pane.
   c. From the list under Authentication methods, select NTLM Agent.
   d. Work with the options of this section to configure NTLM Agent settings.

LDAP digest authentication

The LDAP digest authentication method, which is based on the LDAP authentication method, uses a shared secret known by both sides of the authentication process: a user requesting web access, using a browser on a client of Web Gateway, and Web Gateway.

Web Gateway uses its proxy functions to intercept the request to enable authentication and further filtering under the configured web security policy.

Unlike simpler authentication methods, such as basic authentication, no password is sent directly from the browser to Web Gateway. Instead the password is a part of the shared secret that is known on both sides of the authentication process.
A hash value is calculated for the shared secret and several additional parameters on the client and transmitted to Web Gateway, which calculates the hash again, using its instance of the shared secret, to see if the result is identical. If it is, the user is authenticated.

The hash value that is transmitted from the client to Web Gateway is also referred to as digest. Web Gateway retrieves the shared secret that it requires for recalculating the hash from an LDAP server.

**Calculating a hash for LDAP digest authentication**

The MD5 method for calculating a hash is used when LDAP digest authentication is performed in an authentication process with Web Gateway.

Before the client sends the hash, Web Gateway sends a request for authentication to the client, including a so-called nonce (number only once), which is a number that is randomly created on Web Gateway and is one of the parameters that must be used in addition to the shared secret for calculating the hash.

The complete list of parameters that is used for calculating the hash includes the following:

- User name (part of the shared secret)
- Realm name (part of the shared secret)
- Password (part of the shared secret)
- Nonce
- HTTP request that was sent from the client
- URL of the requested destination in the web

**Configuring LDAP digest authentication on Web Gateway**

LDAP digest authentication on Web Gateway requires the following:

- LDAP authentication must have been configured as the general authentication method on Web Gateway.
- The realm name must be configured as part of the common authentication settings on Web Gateway. This name must also be used for the shared secret.
- You must configure the following parameters for LDAP digest authentication:
  - Enabling of LDAP digest authentication
  - Name of the attribute on the LDAP server that stores the authentication hash
  - Maximum number of times that a nonce can be used
  - Maximum time that a nonce can be used

Optionally, you can do the following.

- Allow only LDAP digest authentication as an authentication method under the current settings
  
  When configuring other authentication settings, you could, however, still allow other authentication methods, for example, the User database method with basic authentication.

- Let a check be performed for the URL that a client sends as a parameter for calculating the hash
  
  This URL should be the same as the URL that this client sends in its request for accessing a particular destination in the web. Otherwise successfully passing digest authentication, based on identical hash values, might allow a user to access a destination that was not requested. So if the result of the check is that both URLs are not the same, the request is blocked.

  As the browsers that are used on clients for sending this information use different URL formats, this check might fail, however, due to the formatting problem, even if two URLs are really the same. For this reason, the URL check is optional.

  The realm name that is used for the shared secret is configured under Common Authentication Parameters, which is a section that is available under every authentication method at the beginning of the Authentication settings.
The parameters for LDAP digest authentication are configured on Web Gateway as part of the settings for the Authentication module (or engine).

When LDAP is selected as the general authentication method at the beginning of these settings, a section named Digest Authentication becomes available after the section for other LDAP specific parameters.

Best practices - Configuring authentication for deployment types

When configuring authentication, you need to consider the type of deployment that is configured for handling the traffic between Web Gateway and its clients, such as the explicit proxy mode or a transparent mode. For each type, there is a rule set in the rule set library that is best suited to handle authentication.

The following two questions are important with regard to the authentication process:

- How are the user credentials that are evaluated during this process obtained by Web Gateway?
  
  This part of the authentication process is sometimes referred to as the authentication front-end.

  The method for obtaining user credentials depends on whether the explicit proxy mode (also known as direct proxy mode) or a transparent mode (transparent router or bridge mode) is configured for handling the traffic between Web Gateway and its clients.

  For the explicit proxy mode, you can configure that clients use a service under the WCCP protocol to send requests as an additional option.

  The rule set library provides suitable rule sets for each of these modes.

- How should credentials be evaluated once they have been obtained?
  
  This is sometimes referred to as the authentication back-end.

  The evaluation of credentials depends on the authentication method that is configured, for example, LDAP or NTLM.

Library rule sets for authentication

The rule sets for configuring authentication are located in the Authentication rule set group of the rule set library.

The following table shows which of these rule sets are recommended for particular types of deployment.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Recommended library rule set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit proxy mode</td>
<td>Direct Proxy Authentication and Authorization</td>
</tr>
<tr>
<td>Transparent router or bridge mode</td>
<td>Authentication Server (Time/IP Based Session)</td>
</tr>
<tr>
<td>Explicit proxy mode with WCCP</td>
<td>If traffic is processed in:</td>
</tr>
<tr>
<td></td>
<td>• Explicit proxy mode — Direct Proxy Authentication and Authorization</td>
</tr>
<tr>
<td></td>
<td>• WCCP mode — Authentication Server (Time/IP Based Session)</td>
</tr>
</tbody>
</table>

After importing a rule set from the library, you can modify its rules to adapt them further to the needs of your network.
Position in the rule sets tree

An authentication rule set should be placed after the Global Whitelist rule set, but before the Common Rules rule set (if you keep these items from the default rule sets tree).

Placing an authentication rule set in this way ensures that a user needs not be authenticated when sending a request for accessing a web object that is on the global whitelist.

Authentication for the explicit proxy mode

When configuring authentication for the explicit proxy mode, a suitable rule set must be implemented on Web Gateway.

Library rule set for the explicit proxy mode

The recommended library rule set for the explicit proxy mode is Direct Proxy Authentication and Authorization. This rule set has two nested rule sets:

- Authenticate with User Database
- Authorize User Groups

When this rule set is implemented, the authentication process is performed for each request that is received from a client of Web Gateway unless an exception rule applies.

Using this rule set is also the preferred way of handling authentication when Citrix is installed or workstations are shared in a configuration.

Direct Proxy Authentication and Authorization rule set

This rule set contains rules for making exceptions that allow a request to be processed on Web Gateway without authenticating the user who sent the request.

Exceptions can be based on:

- The IP address of the client that a request was sent from
- The URL of the web object that is the destination of the request

Using these rules you can ensure that requests coming in from trusted clients or going out to trusted destinations are spared the effort of performing an authentication process for their users, which increases performance.

You can also create rules of your own and add them to this rule set to allow for more exceptions.

Authenticate with User Database nested rule set

This rule set contains a rule that lets authentication be performed for a user who sends a request for web access from a client of Web Gateway. The user is asked to submit credentials, which are evaluated based on information that is stored in the internal user database.

The rule set applies if the user in question has not yet been authenticated and not tried unsuccessfully to authenticate before. The Authentication.Is.Authenticated and Authentication.Failed properties are used to check this.

Instead of using information from the internal user database to evaluate the credentials, you can configure a different authentication method, for example, LDAP or NTLM.
Authorize User Groups nested rule set

This rule set contains a rule that allows only requests of authorized users, which means a request is blocked if the user who sent it is not a member of one of the user groups on a particular list. The request is blocked, even if the user has successfully passed the evaluation that was performed before.

This rule allows you to implement an additional security check. If you want to use it, you need to fill the list that is used in this rule set with user groups. If you do not want to use it, you can disable or delete the rule set.

Modifying the rule set for the explicit proxy mode

When configuring authentication for the explicit proxy mode, you can modify the library rule set to adapt it to the needs of your network.

This includes:

• Changing the authentication method
• Modifying, disabling, or deleting user authorization
• Configuring more exception rules

Changing the authentication method

By default, the method used for evaluating credentials is comparing them to the information stored in the internal user database.

To change this authentication method (authentication back-end), you need to configure the settings that appear next to the Authentication.Authenticate property in the only rule of the Authenticate with User Database rule set.

Under Authentication method, a list of authentication methods is provided to let you select a method that is better suited to the needs of your network, for example, LDAP or NTLM.

Modifying, disabling, or deleting user authorization

The nested Authorized User Groups rule set allows only requests from authorized users. You can fill the list that is provided in the only rule of this rule set with user groups as needed.

If you do not want to use this rule as an additional security check, you can disable or delete the rule set.

Configuring more exception rules

You can add rules to the Direct Proxy Authentication and Authorization rule set to cover more exceptions from the authentication process.

If any of these rules applies, processing of the rule set is stopped, which means it is not executed for the nested rule sets that handle authentication.

For example, you can add a rule to allow requests when the browser on the client they were sent from runs with a particular user agent. Information about the user agent is taken from the request header.

The rule might look as follows:

<table>
<thead>
<tr>
<th>Skip authorization for user agents that are in list Allowed User Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header.Request.Get (&quot;User-Agent&quot;) matches in list Allowed User Agents --&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>

Another rule could allow requests for access to objects on web servers with IP addresses that are on a particular list. The IP address is taken from the URL that was submitted with a request.
This rule might look as follows:

| Skip authorization for destination IPs that are in list Allowed Destination IPs |
| URL.Destination.IP is in range list Allowed Destination IPs --> Stop Rule Set |

**Authentication for transparent modes**

When configuring authentication for the transparent modes, the settings on the browsers that are used for sending requests to Web Gateway need to be modified. A suitable rule must also be implemented on Web Gateway.

**Modifying the browser settings**

To enable authentication for the transparent router or bridge mode, the settings of each web browser that is used for sending requests must be configured to let it trust Web Gateway. If NTLM or Kerberos is also configured as the authentication method on Web Gateway, the authentication process is handled internally, without asking the user to authenticate.

- When using Microsoft Internet Explorer, you need to modify the security settings by:
  - Configuring your local intranet as a security zone
  - Adding Web Gateway as a website to this zone

  This is done by specifying a URL with an IP address or a fully qualified domain name, for example, http://10.10.69.73 or http://*.mcafee.local.

- Configuring automatic logon for all websites in the zone as the security setting for user authentication

  You can configure this under Internet Options, using the Local Intranet and Security Settings - Local Intranet Zone windows.

  If group policies can be configured for a browser, you can also use the Group Policy Management Editor together with the Site to Zone Assignment List and the Logon Options window.

- When using Mozilla Firefox, you need to configure an IP address or a fully qualified domain name for Web Gateway under about:config as the value of the network.automatic-ntlm-auth.trusted-uris parameter, for example, 10.10.69.73 or mwgappl.yourdomain.local.

For more information, refer to the documentation of the respective web browser.

**Library rule set for transparent modes**

The recommended library rule set for the transparent router or bridge mode is Authentication Server (Time/IP Based Session).

It has two nested rule sets:

- Check for Valid Authentication Session
- Authentication Server

Differing from the authentication process that is performed for the explicit proxy mode, this rule set handles authentication by creating an authentication session when a user who sent a request for web access is successfully authenticated.

Subsequent requests that this user sends are processed without requiring authentication again as long as this session is still valid. The default session length is 600 seconds.

Using this rule set in a configuration where Citrix is installed or workstations are shared can lead to the following situation: User A sends a request, is authenticated, and an authentication session is created. Later on, user B sends a request from the same workstation and is still allowed to continue with user A's session.
**Authentication Server (Time/IP Based Session) rule set**
This rule set serves as a container for the two nested rule sets and has no rules of its own.

**Check for Valid Authentication Session nested rule set**
This rule set contains a rule that checks whether a valid session exists for a user who sends a request from a client. Session information is stored in an internal session database. It includes the user name, the IP address of the client, and the session length.

If a valid session exists, processing of the request is continued for the remaining rules and rule sets that are configured. If no valid session exists, the request is redirected to the authentication server.

**Authentication Server nested rule set**
This rule set contains a rule that lets authentication be performed for a user whose request has been redirected to the authentication server. If the authentication was successful, a session is created for this user in the session database.

The method used by default for evaluating the user’s credential is comparing them to the information that is stored in the internal user database. You can replace this method with a different method, for example, LDAP or NTLM.

**Modifying the rule set for transparent modes**
When configuring authentication for transparent modes, you can modify the library rule set to adapt it to the needs of your network.

This includes:
- Modifying the authentication server URL
- Changing the authentication method
- Enabling the ideal conditions rule
- Increasing the session TTL

**Modifying the authentication server URL**
If you have modified the security settings of the browsers that are used for sending requests to Web Gateway by configuring your local domain as a security zone, you can include Web Gateway as a website in this zone by specifying a URL with an IP address or fully qualified domain name for it.

In this case, you also need to modify the URL of the authentication server, which by default contains an IP address for Web Gateway, by inserting the name of your local domain.

The authentication server URL is dynamically generated for an appliance that Web Gateway runs on. As there can be several Web Gateway appliances in a configuration, the IP address cannot be static, but must be configured dynamically, which is done using internal configuration properties.

You can modify this URL under the IP Authentication Server settings, which appear next to the Authentication:Authenticate property in the Redirect clients that do not have a valid session to the authentication server rule of the Check for Valid Authentication Session rule set.

By default, the URL looks like this:

```
http://$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.ip"/>:$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.port"/>
```
Shown in human readable format, a particular authentication server URL could be:

http://10.10.69.71:9090

After adapting the URL to the browser settings that have your local domain configured within a security zone, it looks like this:

http://$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system"/>$.yourdomain.local:$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.port"/>$ with "com.scur.engine.system.proxy.ip"/>$ having been replaced by "com.scur.engine.system"/>$.yourdomain.local.

In human readable format, this could be, for example

http://mwgappl.yourdomain.local:9090

where mwgappl is the host name of an appliance that Web Gateway runs on.

**Changing the authentication method**

By default, the method used for transparent modes to evaluate credentials is comparing them to the information stored in the internal user database.

To change this authentication method (authentication back-end), you need to configure the settings that appear next to the Authentication.Authenticate property in the Authenticate user against user database rule of the Authentication Server rule set.

Under **Authentication method**, a list of authentication methods is provided to let you select a method that is better suited to the needs of your network, for example, LDAP or NTLM.

**Enabling the ideal conditions rule**

The Revalidate session under ideal conditions rule in the Check for Valid Authentication Session rule set lets a user authenticate again under “ideal” conditions, which means authentication will not be asked for at a time when the session has already expired.

In more detail, these conditions are by default:

- The remaining session time is less than 400 seconds.
- The network protocol is HTTP.
- The request that the user sends is a GET request.

Enabling this rule avoids a situation like the following:

1. A user sends a request from a client of Web Gateway and authenticates (600 seconds are allowed for the session time).
2. The user wants to send a ticket to the help desk and begins filling out a data form (300 seconds are used up).
3. The user needs more information to fill out the form and browses the web for this information, which lets some GET requests be received on Web Gateway (200 more seconds are used up).
4. The user completes the data form and submits it, which lets a POST request be received on Web Gateway (200 more seconds elapse, session time expires after the first 100 seconds).
5. As the session time has expired, the user is asked to authenticate again before the POST request is processed. However, due to the session expiration, all filled-out data is lost.
If the ideal conditions rule is enabled, the user is already asked when browsing for information at step 3 to authenticate again, which leaves enough time to complete the form and submit it.

**Increasing the session TTL**

You can increase the allowed time for an authentication session, for example, from the default 600 seconds (10 minutes) to an hour.

You can also modify the time condition in the criteria of the *Revalidate session under ideal conditions* rule, for example, by increasing it from 400 to 600 seconds.

This way, the rule will ask a user, upon receiving a GET request, to authenticate when session expiration is still 10 minutes away.

**Authentication for the explicit proxy mode with WCCP**

Configuring authentication for the explicit proxy mode with WCCP includes import and modification of two rule sets, as well as specifying ports for incoming traffic to trigger the use of the appropriate rule set.

When the explicit proxy mode with WCCP is configured, clients send requests to Web Gateway in explicit proxy mode or using a service under the WCCP protocol.

To handle authentication for the explicit proxy mode, the Direct Proxy Authentication and Authorization rule set is recommended, for the WCCP mode, which is a transparent mode, it is the Authentication Server (Time/IP Based Session) rule set.

This means you should import both rule sets and complete additional activities as needed for both modes, including the modification of the browser settings for the WCCP mode.

To let traffic for each mode be handled by the appropriate authentication rule set, you can configure different ports for both types of traffic and specify the respective port in the criteria of each rule set.

**Configuring different ports for the explicit proxy and WCCP modes**

The ports for the explicit proxy and WCCP modes could, for example, be 9090 and 9091. You need to specify the port for the WCCP mode when configuring a WCCP service and both ports in the list of HTTP ports.

A WCCP service is configured by entering it in the *WCCP Services* list. This list appears after selecting *WCCP* in the Transparent Proxy section of the Proxies (HTTP(S), FTP, ICAP, and IM) system settings.

The section appears within these settings when you begin to configure the explicit proxy mode with WCCP by selecting *Proxy (optional WCCP)* under Network Setup.

The entry for a WCCP service that is used for traffic coming in on port 9091 could, for example, look as follows:

<table>
<thead>
<tr>
<th>No</th>
<th>Service ID</th>
<th>WCCP router ...</th>
<th>Ports ...</th>
<th>Proxy listener ...</th>
<th>MDS ...</th>
<th>Assignment</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>91</td>
<td>10.10.69.7</td>
<td>80, 443</td>
<td>false</td>
<td>10.10.69.73</td>
<td>9091</td>
<td>oooooo 1000</td>
</tr>
</tbody>
</table>

The HTTP Port Definition List can be configured in the HTTP Proxy section, which is located below the Transparent Proxy section.

The entries for the explicit proxy and WCCP modes could look as follows:

<table>
<thead>
<tr>
<th>No</th>
<th>Listener address</th>
<th>Serve ...</th>
<th>Ports ...</th>
<th>Transparent ...</th>
<th>McAfee ...</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0:9090</td>
<td>true</td>
<td>443</td>
<td>false</td>
<td>true</td>
<td>Explicit proxy traffic</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.0:9091</td>
<td>true</td>
<td>443</td>
<td>false</td>
<td>true</td>
<td>WCCP traffic</td>
</tr>
</tbody>
</table>
Adapting the criteria of the authentication rule sets

After configuring different ports for traffic coming in under the explicit proxy mode or using a WCCP service, for example, 9090 and 9091, you need to adapt the criteria of the rule sets for handling the two kinds of traffic.

The adapted rule criteria of the Direct Proxy Authentication and Authorization rule set would then look as follows:

Proxy.Port equals 9090 AND (Connection.Protocol equals "HTTP" OR Connection.Protocol equals "HTTPS")

For the Authentication Server (Time/IP Based Session) rule set, the adapted criteria would be:

Proxy.Port equals 9091

Best practices - Configuring LDAP authentication

LDAP authentication is one of the methods that can be configured on Web Gateway for authenticating users. LDAP stands for Lightweight Directory Access Protocol. Under this protocol, the authentication process on Web Gateway can be integrated with an existing directory service in a network. The directory holds user information, which can be queried and used for authentication.

In addition to authenticating a user, a directory can be queried to find other pieces of information about a user and the groups that a user belongs to. These pieces of information are called attributes.

An entry for a user in, for example, the Microsoft Windows Server Active Directory (Active Directory) usually includes a memberOf attribute holding information about the groups that the user belongs to. An entry for a group usually has a member attribute to hold the group members' user names.

The results returned by lookups for both user and group attributes are stored on Web Gateway as the value of the Authentication.UserGroups property.

LDAP authentication process

The process that integrates user authentication on Web Gateway and a directory on an LDAP server includes the following main steps.

• Web Gateway sends an initial bind request with administrator credentials to the LDAP server.

• If the request is successful, Web Gateway sends a query with the user name that the user submits.

  The purpose of this query is to find a distinguished name that the user name is mapped to in the directory on the LDAP server.

• If a distinguished name is found, the LDAP server sends it back.

  The distinguished name (DN) is a combination of information about a user, a user group, and a network domain provided in an LDAP-style syntax.

  For example, for the user name jsmith, the LDAP server sends back the distinguished name cn=John Smith, cn=users, dc=ldap, dc=local.

• Web Gateway sends a second bind request to the LDAP server with the purpose of authenticating the user.

  This request includes the distinguished name and the password that the user submitted.

• If the request is successful, the user is authenticated.

You can record the steps of the authentication process in a tcpdump to review them.
**Rule for authenticating a user under LDAP**

To configure LDAP authentication on Web Gateway, you must implement a rule that authenticates a user in an integrated process with Web Gateway and a directory on an LDAP server.

The rule set library provides a rule set with a default rule that you can modify and use for this purpose. The modified rule looks as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Authenticate with LDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate&lt;LDAP&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Authenticate&lt;Default&gt;</td>
</tr>
</tbody>
</table>

The rule applies if a user has not yet been authenticated using the LDAP authentication method.

The settings of the Authentication.Authenticate property in this rule are configured to provide the information that is necessary to run the authentication process successfully, including the IP address of the LDAP server and the administrator credentials for Web Gateway.

**Configure the LDAP method for authenticating a user**

To configure the LDAP method for authenticating a user, you can adapt an already existing authentication rule. Modify the names and settings within this rule in a way that makes them suitable for LDAP authentication.

**Task**

1. Import the Explicit Proxy Authentication and Authorization rule set from the rule set library.
   
   This rule set is for authentication in explicit proxy mode. For a transparent mode, import the Authentication Server rule set.

2. Adapt the authentication rule in the nested Authenticate with User Database rule set to make it suitable for LDAP authentication.

   For a transparent mode, adapt the authentication rule in the nested Authentication Server rule set.

   a. Rename the current rule name to Authenticate with LDAP.
   
   b. Rename the settings of the Authentication.Authenticate property to a name that is appropriate for LDAP-related settings, for example, LDAP.
   
   c. Modify the settings to make them suitable for LDAP authentication.

3. Rename the nested rule set to Authenticate with LDAP.

   Instead of adapting the nested library rule set, you can also disable or delete it and create a new nested rule set for LDAP authentication.

   The second nested rule set of the Explicit Proxy Authentication and Authorization library rule set, Authorize User Groups, is not needed for LDAP authentication.

   If you delete this nested rule set, you should rename the nesting rule set or have only one rule set named, for example, Explicit Proxy Authentication with LDAP.

4. Click Save Changes.
Configure the settings for the LDAP authentication method

Configure the settings for the LDAP authentication method by modifying the settings in the rule for authenticating a user that you have imported from the rule set library.

**Task**

1. In the imported rule, click the settings of the **Authentication.Authenticate** property that you have renamed to **LDAP** or a similar name.

   The **Edit Settings** window opens.

2. Under **Authentication Method**, select **LDAP**.

   The **LDAP Specific Parameters** section appears next to **Common Authentication Parameters**.

   You can leave the common parameters as they are, as well as the **LDAP**-specific parameters that are not mentioned in the following.

3. In the **LDAP server(s) to connect to** list, add an entry for the LDAP server that the directory with the user information resides on.

   The syntax for an entry is as follows:

   `{LDAP | LDAPS}://<IP address>[:<port number>]`

   For example: `LDAP://10.205.67.8:389`

   LDAP is an insecure protocol, as it transmits information in clear text. We recommend using LDAPS (secure LDAP) if possible.

   The default LDAP port is 389 while LDAPS uses 636.

4. Provide the administrator credentials that Web Gateway submits when trying to connect to the LDAP server.

   a. Under **Credentials**, type a common name and a domain controller name in LDAP style, for example:

      `cn:administrator,cn:users,dc:ldap,dc:local`

   b. Under **Password**, type an administrator password.

5. If the directory on the LDAP server is an Active Directory, deselect **Allow LDAP directory to follow referrals**.

6. Provide information for the query to find the distinguished name of the user who is to be authenticated.

   a. Under **Base distinguished name to user objects**, specify a starting point for the query.

      The starting point is specified in LDAP style, for example:

      `cn:users,dc:ldap,dc:local`

   b. Select **Map user name to DN**.

      Selecting this option lets the query search for a distinguished name that the submitted user name is mapped to in the directory.
Under **Filter expression to locate a user object**, specify a user attribute that allows the distinguished name to be found.

Specifying this filter expression enables the search to find the entry for a user in the directory. The filter expression is the user name that the user submitted. The user name is stored in the directory as the value of an attribute that is part of the entry for a user.

In an Active Directory, the name of the attribute that stores the user name is `sAMAccountName`. On Web Gateway, the user name is stored in a variable named `%u`.

The filter expression must therefore be specified as follows if an Active Directory is used:

```
samaccountname=%u
```

Using this filter expression, the query will find the user entry and, consequently, try to map the user name to a distinguished name that might have been entered into the directory for a user with that user name.

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

8 Click **Save Changes**.

These settings enable Web Gateway to authenticate a user under the LDAP authentication method. To retrieve information stored in other attributes within a directory, additional settings are required.

**Configure queries for user and group attributes**

Configure additional settings to perform queries that retrieve ("pull") more information about users and user groups from a directory on an LDAP server.

The settings for these queries are part of the settings that you configure for the Authentication module (engine) on Web Gateway to handle the integrated process for authenticating a user.

**Task**

1 Configure a query for user attributes.
   
   a Select **Get user attributes**.

   You need not configure any special values for the **Base distinguished name to user objects** option, as these values are the same as those that you already configured for the purpose of authenticating a user.

   b In the **User attributes to retrieve** list, add the name of the attribute that the query should find a value for. You can also add multiple names here.

   For example, to retrieve information about the group or groups that a user belongs to, add `memberof`.

   c Under **Attributes concatenation string**, type a character for separating multiple resulting values, for example, a comma.

2 Configure a query for group attributes.
   
   a Select **Get group attributes**.

   b Under **Base distinguished name to group objects**, provide a starting point for the query using LDAP syntax, for example, `ou=groups,dc=ldap,dc=local`.

   c Under **Filter expression to locate a group object**, specify an attribute of a group that allows the group to be found.

   For example, specify `memberof=%u`, which has `memberof` as the attribute name and the `%u` variable that holds the user’s user name on Web Gateway as the attribute value.
In the **Group attributes to retrieve** list, add the name of the attribute that the query should find a value for. You can also add multiple names here.

For example, to find the so-called common name of a group, add `cn`.

Under **Attributes concatenation string**, type a character for separating multiple resulting values, for example, a comma.

### Storing an attribute in a separate property

You can store a user or group attribute in a separate User-Defined property for logging and other purposes. When a query for an attribute of a user or user group is performed in a directory on an LDAP server, the resulting information is stored on Web Gateway as the value of the `Authentication.UserGroups` property.

If you are interested in a particular piece of information, for example, the email address of a user, you can also retrieve it separately and store it in a User-Defined property.

For this purpose, you must create an additional rule, as well as additional settings named, for example, `LDAP Email Lookup`, for the Authentication module (engine). In this rule, the Authentication module runs with the additional settings to retrieve the information that is stored within the entry for a user as the value of the email attribute.

Options must be especially configured in the additional settings as follows:

- **Get user attributes** must be enabled.
- The **User attributes to retrieve** list must contain a single entry for the email attribute. When an Active Directory is running on the LDAP server, the attribute name is `mail`.
- **Map user to DN** must be disabled.

Not disabling the option produces an error, as the user name has already been mapped when the Authentication module was running with the LDAP settings to authenticate the user.

All other options can be configured in the same way as the settings within the rule that authenticates the user.

The complete rule should look as follows:

**Name**

**Get email information and store separately**

**Criteria**

```
Authentication.IsAuthenticated equals true AND
Authentication.GetUserGroups <LDAP_Email_:Lookup> does not contain "no-group"
```

**Action**

```
-> Continue
```

**Event**

```
Set User-Defined.Email=
List.OfString.ToString
(Authentication.UserGroups," ")
```

The rule must be added to the rule set for LDAP authentication and placed after the rule that authenticates the user.

### Storing the original user name for logging

The original user name can be stored for logging purposes.

When a user has been authenticated using the LDAP method, the value of the `Authentication.Username` property is set to the user’s distinguished name. If the property is used for creating a log entry, the part of the log entry that identifies the user will look, for example, as follows:

```
CN=John Smith,CN=Users,DC=LDAP,DC=local
```
To let the log entry show the original user name, which might be `jsmith`, rather than the distinguished name, you can modify the rule set for LDAP authentication in a suitable manner.

Instead of having only a rule that authenticates a user under LDAP, the rule set should contain the following:

- A rule that handles LDAP authentication for a user and stores the original user name in a User-Defined property
- One or more rules that perform other LDAP-related activities, for example, retrieving information about the group that a user belongs to
- A rule that restores the original user name as the value of the Authentication.Username property after all LDAP-related activities have been completed

**Rule for authenticating a user and storing the user name**

The following rule stores the original user name after authenticating the user. An event in this rule sets the value of a User-Defined property accordingly.

Name

**Authenticate user and store user name**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
</table>

The user name is retrieved by querying the directory on the LDAP server for this name. The settings of the `Authentication.Authenticate` property, which is responsible for authenticating the user, are configured accordingly.

When the query has been performed, the user name is stored as the value of the `Authentication.Groups` property. It is converted into a string, using the `List.OfString.ToString` property.

> The original value of the converted property is a list of strings, as it might include not only the user name, but also other pieces of information, after all LDAP-related activities have been completed.

**Rule for retrieving user group information**

The following rule is an example for an additional LDAP-related activity. It retrieves information about the groups that a user belongs to.

Name

**Get user group information**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Authentication.IsAuthenticated equals true</code> AND <code>Authentication.GetUserGroups&lt;LDAP_Group_:Lookup&gt; does not contain &quot;no-group&quot;</code></td>
<td>Continue</td>
</tr>
</tbody>
</table>
To identify the user, the rule still needs to know the user's distinguished name, so the original user name cannot yet be restored as the value of the Authentication.UserName property.

You must create different settings and configure them for the Authentication module (engine) to run and retrieve a value for the Authentication.GetUserGroups property.

The name of these settings might, for example, be LDAP Group Lookup, as in this sample rule.

Within these settings, the Map user to DN option must be disabled.

**Rule for restoring the original user name**

The following rule restores the original user name as the value of the Authentication.UserName property.

**Name**

**Restore user name**

**Criteria**

| Authentication.Authenticate<LDAP> equals false |

| Action | Event |

| Stop Rule Set | Set Authentication.UserName= User-Defined.Authentication.Username |

An event in this rule sets this property to the value of the User-Defined property that you created to store the original user name in a preceding rule. The distinguished name that has temporarily been the value of this property is overwritten.

When the original user name has been restored, the property can be used for logging purposes.

**Testing and troubleshooting LDAP authentication**

Several activities can be completed for testing and troubleshooting the LDAP authentication process.

A tool for testing the configured authentication process with a given user name and password is available on the user interface of Web Gateway.

If running the tool shows that the process failed, carefully review what you have configured. If no errors can be found, you can create a debug log using another tool. If this does not explain the failure either, create a tcpdump using a third tool.

**Test authentication for a given user name and password**

The settings for the Authentication module include a section for testing purposes. You can enter a user name and password and let Web Gateway attempt to authenticate the user.

**Task**

1. Select Policy | Settings.
2. On the Engines branch of the settings tree, click the settings for the Authentication module (engine) that you have modified or newly created, for example, the LDAP settings.
   Otherwise no changes in the directory on the LDAP server are detected until the cache expiration time has elapsed.
4. Expand Authentication Test and type a user name and password in the fields that are provided.
5. Click Authenticate User.
The result of the authentication process is shown under **Test result**.

- If the process is successfully performed, an OK message appears.
  The testing tool also displays any attribute values that you have configured queries for.
- If the process fails, the following message appears: **Error: Authentication failed.**

**Create a debug log file for troubleshooting authentication**

You can create a debug log file to record the authentication process and review it for troubleshooting purposes.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance that you want to create a debug log file on, then click **Troubleshooting**.
3. In the **Authentication Troubleshooting** section, select **Log authentication events**.

   **i** We recommend that you also select **Restrict tracing to one IP** and specify a client IP address to prevent the log file from becoming too large.

4. Reproduce the authentication process.
   A debug log file is created for the process.
5. Locate the debug log file.
   a. Select **Troubleshooting**
   b. On the troubleshooting tree, select the appliance that you created the debug log file on, then click **Log files**.
   c. Open the **debug** folder and look for the **mwg-core.Auth.debug.log** file with the appropriate time stamp.

   The log file contains log lines showing failure IDs for the authentication process. The meaning of these IDs is as follows:

   - 0 – **NoFailure**: Authentication was successful
   - 2 – **UnknownUser**: Cannot map user name to user DN
   - 3 – **WrongPassword**: Bind with user password failed
   - 4 – **NoCredentials**: Credentials are missing or have invalid format
   - 5 – **NoServerAvailable**: Could not get a server connection
   - 6 – **ProxyTimeout**: Request is being processed longer than the configured timeout
   - 8 – **CommunicationError**: Communication with server failed, for example, due to a timeout

**Create a tcpdump for troubleshooting authentication**

If the reason for a failed authentication process cannot be found by reviewing a debug log file, create a tcpdump to retrieve more information.

**Task**

1. Select **Troubleshooting**.
2. On the troubleshooting tree, select the appliance that you want to create a tcpdump on, then click **Packet tracing**.
3 In the **Command line parameters** field, type the following:

```
-s 0 -i any port 389
```

The port parameter lets Web Gateway connect to the LDAP server over an unencrypted port, which is required for troubleshooting purposes.

4 Click **tcpdump start**.

5 Reproduce the problem, then click **tcpdump stop**.

6 Open the trace using the **wireshark** tool. Then work with the **ldap.bindResponse** display filter to find a response from the LDAP server.

The server response usually includes LDAP, Active Directory, and other error codes. For example, in the following line from a server response:

```
"invalidCredentials (80090308: LdapErr: DSID-0c09030f, comment: AcceptSecurityContext error, data 773, vece)"
```

the 773 error code is an Active Directory error code meaning that the user password must be changed.

---

## 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 authentication.
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

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*.

---

**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*.

---

**IM Authentication rule set**

The IM Authentication rule set is a library rule set for instant messaging authentication.

<table>
<thead>
<tr>
<th>Library rule set – IM Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Nested library rule set – IM Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsServerRequest equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – IM Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Connection.Protocol.IsIM equals true AND IM.MessageCanSendBack is true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

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.

---

**One-time passwords**

One-time passwords (OTPs) can be processed on Web Gateway to authenticate users. This includes the use of passwords for authorized overriding when a web session has terminated due to quota expiration.

When a user sends a request for web access, authentication is first performed using one of the other authentication methods that are available on Web Gateway, for example, authentication based on information stored in the internal user database.

If the use of one-time passwords is configured, this authentication method is performed as a second step. Web Gateway informs the user that a one-time password is also needed for web access and upon the user's request for such a password, it forwards the user name to a McAfee® One Time Password (McAfee OTP) server and asks the server to provide a password.

If the request is granted, the McAfee OTP server returns a one-time password, which is, however, not exposed to Web Gateway. In its response, the McAfee OTP server also includes what is called “context” information in a header field.

The context information lets the password field and submit button in the page that was presented to the user be activated, so the user can click the button, which submits the one-time password and lets the user access the requested web object.

To implement the use of one-time passwords on Web Gateway, you can import a rule set from the rule set library. After importing the rule set, default settings are provided, which you can configure to adapt them to the needs of your network.
The settings that need to be configured include the IP address or host name of the McAfee OTP server and the port on this server that listens to requests from Web Gateway.

A user name and password for Web Gateway to authenticate to the McAfee OTP server are also required.

If the communication between Web Gateway and the McAfee OTP server should be SSL-secured, you need to import a certificate for use in this communication.

The McAfee OTP server must be configured for working with Web Gateway to handle the authentication process.

**One-time passwords for authorized overriding**

When quota restrictions are imposed on web usage from within your network, a one-time password can be used as the password that is required to override the termination of a web session due to quota expiration.

To implement the use of one-time passwords for authorized overriding, you can import a different rule set from the library, which also allows you to configure the settings for the authentication process.

**Using one-time passwords from a McAfee Pledge device**

One-time passwords for authenticating users or performing an authorized override can be provided by a McAfee® Pledge device.

To enable this method of using one-time passwords for the authentication process, you need to implement suitable rule sets, which you can import from the rule set library. Settings for the authentication process are implemented with the import.

For more information on working with a McAfee Pledge device, refer to the documentation for this product.

**Configure one-time passwords for authenticating users**

To configure the use of one-time passwords for authenticating users, complete the following high-level steps.

**Task**

1. Import the *Authentication Server (Time/IP Based Session with OTP)* rule set from the rule set library.
   - When using one-time passwords from a McAfee Pledge device, import the *Authentication Server (Time/IP Based Session with OTP and Pledge)*
     - The rule sets are located in the *Authentication* rule set group.

2. Configure the settings for one-time passwords.

3. Save your changes.

For information on how to configure the McAfee OTP server for working with Web Gateway, refer to the McAfee OTP server documentation.

**Configure one-time passwords for authorized overriding**

To configure the use of one-time passwords for authorized overriding, complete the following high-level steps.

**Task**

1. Import the *Authorized Override with OTP* rule set from the rule set library.
   - When using one-time passwords from a McAfee Pledge device, import *Authorized Override with OTP and Pledge*.
     - The rules sets are located in the *Coaching/Quota* rule set group.
2 Configure the settings for one-time passwords.

3 Save your changes.

For information on how to configure the McAfee OTP server for working with Web Gateway, refer to the McAfee OTP server documentation.

**Configure the settings for one-time passwords**

Settings for one-time passwords are implemented with default values after importing the rule sets that handle the use these passwords. Configure these settings to adapt them to the requirements of your network.

You need to configure different settings for authentication and authorized overriding with one-time passwords.

**Task**

1 Select Policy | Settings.

2 On the Engines branch of the settings tree, expand Authentication.

3 To configure settings for using one-time passwords to authenticate users, complete the following substeps. Otherwise continue with step 4.

   a Click OTP.
   
   The OTP settings appear on the settings pane.

   b Configure the settings in the One-Time Password Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

   c Click IP Authentication Server.
   
   The IP Authentication Server settings appear on the settings pane.

   d Configure the settings in the IP Authentication Server Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

   e Click User Database at Authentication Server.
   
   The User Database at Authentication Server settings appear on the settings pane.

   f Configure the settings in the User Database Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.
   
   Then continue with step 5.

4 To configure settings for using one-time passwords in authorized overriding, complete the following substeps.

   a Click OTP.
   
   The OTP settings appear on the settings pane.

   b Configure the settings in the One-Time Password Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

5 Click Save Changes.
Authentication Server (Time/IP Based Session with OTP) rule set

The Authentication Server (Time/IP Based Session with OTP) rule set is a library rule set that enables the use of one-time passwords for authenticating users.

<table>
<thead>
<tr>
<th>Library rule set – Authentication Server (Time/IP Based Session with OTP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- Check for Valid Authentication Session
- Authentication Server

Check for Valid Authentication Session

This nested rule redirects a user's request sent from a client to the authentication server if the user has not yet been successfully authenticated on that server.

<table>
<thead>
<tr>
<th>Nested library rule set – Check for Valid Authentication Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsServerRequest equals false AND</td>
</tr>
<tr>
<td>(Connection.Protocol equals &quot;HTTP&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;SSL&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;HTTPS&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;IFP&quot;)</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies if the request that is currently processed is not requesting a connection to the authentication server and the protocol used in this communication is one of the four that are specified.

The rule set contains the following rules:

**Fix hostname**


The rule uses an event to set the host name that is submitted with the URL of a request to a particular value, which is required when communication is going on under the SSL protocol. This value is the common name of the certificate that is provided in this communication.

The rule applies if the request that is processed contains the CERTVERIFY command and no wildcards are allowed for the common name.

**Redirect clients that do not have a valid session to the authentication server**

*Authentication.Authenticate<IP Authentication Server> equals false AND Command.Name does not equal "CONNECT"* → Authenticate<Default>

The rule uses the Authentication.Authenticate property to check whether the user who sends a request is successfully authenticated at the user database of the authentication server. For this purpose, the IP address of the client that the request was sent from is evaluated.

The Command.Name property is used to check whether the request is a connection request in SSL-secured communication.

If neither is the case, the user is asked to submit credentials for authentication. This action is executed with the specified settings.
Revalidate session under ideal conditions

Authentication.CacheRemainingTime less than 400 AND
Connection.Protocol equals "HTTP" AND
Command.Name equals "GET"

-> Authenticate<Default>

Under particular conditions (which could be termed "ideal"), a user is asked to authenticate again after sending a request to ensure the current web session is prolonged before the time quota has elapsed completely.

This is done if communication is going on under the HTTP protocol and the request contains the GET command.

The rule is not enabled by default.

Authentication Server

This nested rule set forwards a request for web access when a user submitted a valid one-time password. A user who could not submit a valid one-time password is asked to authenticate.

Authentication is first performed using information from the user database on an authentication server. A successfully authenticated user is then informed that web access also requires a one-time password, which is sent by Web Gateway upon the user's request.

<table>
<thead>
<tr>
<th>Nested library rule set – Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsServerRequest equals true</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user who sent a request must be authenticated using information from an authentication server.

The rule set contains the following rules:

Redirect if we have a valid OTP

Authentication.Authenticate<OTP> equals true -> Redirect <Redirect Back from Authentication Server>

The rule uses the Authentication.Authenticate property to check whether a user who submitted a one-time password with a request for web access could be successfully authenticated.

If this is the case, web access is allowed and the user is redirected from the authentication server to the requested web object.

Stop after providing an invalid OTP

Authentication.Failed equals true -> Block<Authorized Only>

The rule uses the Authentication.Failed property to check whether a user who submitted a one-time password with a request for web access could not be successfully authenticated.

If this is the case, the request is blocked and a message informs the user about the blocking and the block reason.

Authenticate user against user database

Authentication.Authenticate<User Database at Authentication Server> equals false -> Authenticate<Default>

The rule uses the Authentication.Authenticate property to check whether a user who sent a request and submitted an invalid one-time password could be successfully authenticated at the user database on the authentication server.

If this is not the case, the user is asked to authenticate.
Send OTP if requested

*Header.Exists(Request.OTP) equals true -> Continue – Authentication.SendOTP<OTP>*

If none of the preceding rules in this rule set has applied, it means no valid one-time password was submitted by a user who sent a request for web access, but authentication at the user database on the authentication server was successful.

Then this rule is processed, which uses the `Header.Exists` property to check whether the request has a header providing the information that sending a one-time password is requested.

If this is the case, the rule uses an event to send a one-time password to the user.

Return authentication data to client


The rule uses the `Header.Exists` property to check whether there is a header in a request with information that sending a one-time password is requested.

If this is the case, the request is blocked and a message sent to inform the user who sent the request that a one time password is required for access.

An event is also triggered that adds a header with context information about the one-time password authentication process to the block message.

The first of the two event parameters specifies the header information that is added. The second parameter is a property that has information about the one-time password authentication process as its value, which is the source of the added information.

Block request and offer sending OTP

*Always -> Block<Authentication Server OTP>*

If none of the preceding rules in this rule set have applied, the Block action of this rule is always executed.

The action stops rule processing and the request is not forwarded.

The action settings specify that a message is sent to inform the user that a one-time password is required for web access, which can be obtained from Web Gateway.

Authorized Override with OTP rule set

The Authorized Override with OTP rule set is a library rule set for enabling the use of one-time passwords in authorized overriding.

<table>
<thead>
<tr>
<th>Library rule set – Authorized Override with OTP and Pledge</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – SSL.ClientContext.IsApplied equals true OR Command.Name does not equal &quot;CONNECT&quot;</td>
</tr>
<tr>
<td><strong>Cycles</strong> – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule criteria specified that the rule set applies when SSL-secured communication is configured or the request that is currently processed is not a CONNECT request, which is usually sent at the beginning of this communication.

The following rule sets are nested in this rule set:

- Verify OTP
- OTP Needed?

Verify OTP

This nested rule checks whether a user who sends a one-time password with a request for authorized overriding is successfully authenticated and performs a redirect to the requested web object if this is true.
Nested library rule set – Verify OTP

Criteria – Quota.AuthorizedOverride.IsActivationRequest.Strict<Default> equals true
Cycles – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request to override the termination of a web session due to quota expiration and to continue with the session.

The rule set contains the following rules:

Verify OTP

Authentication.Authenticate<OTP> equals false -> Block<Authorized Only>

The rule uses the Authentication.Authenticated property to check whether the user who submitted a one-time password when sending an authorized overriding request has been successfully authenticated.

If this is not the case, the request is blocked and the user is informed about the blocking and the reason for it.

The Block action is executed with the specified settings.

The session is validated. Redirect to the original page

Always -> Redirect<Default>

If authentication of a user who submitted a one-time password with a request for authorized overriding did not fail, the preceding rule in this rule set does not apply and processing continues with this rule.

The rule always allows the user to continue with the current session and performs a redirect to the requested web object.

The Redirect action is executed with the specified settings.

OTP Needed?

This nested rule set provides a one-time password for a user who sends a request for authorized overriding if the requested web object is located on a host within the corporate domain of McAfee.

Nested library rule set – OTP Needed?

Criteria – URL.Host matches *mcafee.com*
Cycles – Requests (and IM)

The rule set criteria specifies that the rule set applies when the host of the URL sent in a request is located within the corporate domain of McAfee.

The rule set contains the following rules:

Send OTP if requested

Header.Exists(Request.OTP) equals true -> Continue – Authentication.SendOTP<OTP>

If none of the proceeding rules in this rule set have applied when processing a request, it means no valid one-time password was submitted by the user who sent the request, but authentication at the user database of the authentication server was successful.

Then this rule is processed, it uses the Header.Exists property to check whether the request has a header providing the information that sending a one-time password is requested.

if this is the case, an event is triggered that send a one-time password to the user.

Return authentication data to client


The uses the Header.Exists property to check whether the request has a header providing the information that sending a one-time password is requested.
If none of the proceeding rules in this rule set have applied when processing a request, it means no valid one-time password was submitted by the user who sent the request, but authentication at the user database of the authentication server was successful.

If this is the case, the request is not forwarded and an event is triggered that sets a particular property to a value that provides information about the authentication of the user.

The Block action is executed with the specified settings, which require that a message is sent to inform the user about the reason of the blocking.

The information that the event provides is specified by the OTP:Context event parameter. The property that has its value set to this information is specified in a second parameter.

**Block request and offer sending OTP**

*Always -> Block<Authentication Server OTP>*

If none of the preceding rules in this rule set have applied when processing a request, the action of this rule is always executed.

It stops rule processing and the request is not forwarded. The action settings specify that a message is sent to inform the user that a one-time password can be obtained from Web Gateway.

**Authentication Server (Time/IP Based Session with OTP and Pledge) rule set**

The Authentication Server (Time/IP Based Session with OTP and Pledge) rule set is a library rule set for authenticating users through one-time passwords that are provided by a McAfee Pledge device.

```
| Library rule set – Authentication Server (Time/IP Based Session with OTP and Pledge) |
|---------------------------|---------------------------------------------|
| Criteria – *Always*        |
| Cycle – Requests (and IM)  |
```

The following rule sets are nested in this rule set:

- *Check for Valid Authentication Session*
- *Authentication Server*

**Check for Valid Authentication Session**

This nested rule redirects a user's request sent from a client to the authentication server if the user has not yet been successfully authenticated on that server.

```
<table>
<thead>
<tr>
<th>Nested library rule set – Check for Valid Authentication Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsServerRequest equals false AND</td>
</tr>
<tr>
<td>(Connection.Protocol equals &quot;HTTP&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;SSL&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;HTTPS&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;IFP&quot;)</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>
```

The rule set criteria specifies that the rule set applies if the request that is currently processed is not requesting a connection to the authentication server and the protocol used in this communication is one of the four that are specified.
The rule set contains the following rules:

**Fix hostname**

\[\text{Command.Name equals "CERTVERIFY" AND SSL.Server.Certificate.CN.HasWildcards equals false} \implies \text{Continue – Set URL.Host = SSL.Server.Certificate.CN}\]

The rule uses an event to set the host name that is submitted with the URL of a request to a particular value, which is required when communication is going on under the SSL protocol. This value is the common name of the certificate that is provided in this communication.

The rule applies if the request that is processed contains the CERTVERIFY command and no wildcards are allowed for the common name.

**Redirect clients that do not have a valid session to the authentication server**

\[\text{Authentication.Authenticate\langle IP Authentication Server\rangle equals false AND Command.Name does not equal "CONNECT"} \implies \text{Authenticate\langle Default\rangle}\]

The rule uses the Authentication.Authenticate property to check whether the user who sends a request is successfully authenticated at the user database of the authentication server. For this purpose, the IP address of the client that the request was sent from is evaluated.

The Command.Name property is used to check whether the request is a connection request in SSL-secured communication.

If neither is the case, the user is asked to submit credentials for authentication. This action is executed with the specified settings.

**Revalidate session under ideal conditions**

\[\text{Authentication.CacheRemainingTime less than 400 AND Connection.Protocol equals "HTTP" AND Command.Name equals "GET"} \implies \text{Authenticate\langle Default\rangle}\]

Under particular conditions (which could be termed "ideal"), a user is asked to authenticate again after sending a request to ensure the current web session is prolonged before the time quota has elapsed completely.

This is done if communication is going on under the HTTP protocol and the request contains the GET command.

The rule is not enabled by default.

**Authentication Server**

This nested rule set forwards a request for web access by a user who submitted a valid one-time password that was retrieved from a McAfee Pledge device.

A user who did not submit a valid one-time password is asked to authenticate. Authentication is first performed using information from the user database of the authentication server.

A successfully authenticated user is then informed that web access also requires a one-time password from a McAfee Pledge device.

<table>
<thead>
<tr>
<th>Nested library rule set - Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – Authentication.IsServerRequest equals true</td>
</tr>
<tr>
<td><strong>Cycle</strong> – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user who sent a request must be authenticated using information from an authentication server.
The rule set contains the following rules:

**Authenticate user against user database**

Authentication.Authenticate(User Database at Authentication Server) equals false -> Authenticate<Default>

The rule uses the Authentication.Authenticate property to check whether a user who sent a request and submitted an invalid one-time password could be successfully authenticated at the user database on the authentication server.

If this is not the case, the user is asked to authenticate.

**Show block template**

URL.GetParameter(pledgeOTP) equals " " -> Block<Authentication.Server OTP with PledgeOTP>

The rule uses the URL.GetParameter property to check whether a one-time password from a McAfee Pledge device was sent as a parameter of the URL in a request.

If the parameter is empty, the request is blocked and the user is informed that authentication using a one-time password from a McAfee Pledge device is also required for web access.

**Retrieve OTP context**

Always -> Continue – Authentication.SendOTP<OTP>

The rule uses an event to send context information on the one-time password authentication process to an authenticated user.

This way the information is retrieved that is required to validate a one-time password on a McAfee OTP server.

**Redirect back if we have a valid OTP**

Authentication.Authenticate<OTP> equals true -> Redirect<Redirect Back from Authentication Server>

The rule uses the Authentication.Authenticate property to check whether a user who submitted a one-time password with a request for web access could be successfully authenticated.

If this is the case, web access is allowed and the user is redirected from the authentication server to the requested web object.

**Stop after providing an invalid OTP**

Authentication.Failed equals true -> Block<Authorized Only>

The rule uses the Authentication.Failed property to check whether a user who submitted a one-time password with a request for web access could not be successfully authenticated.

If this is the case, the request is blocked and a message informs the user about the blocking and the block reason.

**Authorized Override with OTP and Pledge rule set**

The Authorized Override with OTP and Pledge rule set is a library rule set for authorized overriding using one-time passwords that are provided by a McAfee Pledge device.

<table>
<thead>
<tr>
<th>Library rule set – Authorized Override with OTP and Pledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – SSL.ClientContext.IsApplied equals true OR Command.Name does not equal &quot;CONNECT&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule criteria specified that the rule set applies when SSL-secured communication is configured or the request that is currently processed is not a CONNECT request, which is usually sent at the beginning of this communication.

The following rule sets are nested in this rule set:
• Verify OTP
• OTP Needed?

Verify OTP
This nested rule checks whether a user who sends a one-time password with a request for authorized overriding is successfully authenticated and performs a redirect to the requested web object if this is true.

<table>
<thead>
<tr>
<th>Nested library rule set – Verify OTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <code>Quota.AuthorizedOverride.IsActivationRequest.Strict&lt;Default&gt;</code> equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request to override the termination of a web session due to quota expiration and to continue with the session.

The rule set contains the following rules:

Verify OTP

Authentication.Authenticate<OTP> equals false → Block<Authorized Only>

The rule uses the `Authentication.Authenticated` property to check whether the user who submitted a one-time password when sending an authorized overriding request has been successfully authenticated. If this is not the case, the request is blocked and the user is informed about the blocking and the reason for it. The Block action is executed with the specified settings.

The session is validated. Redirect to the original page

Always → Redirect<Default>

If authentication of a user who submitted a one-time password with a request for authorized overriding did not fail, the preceding rule in this rule set does not apply and processing continues with this rule. The rule always allows the user to continue with the current session and performs a redirect to the requested web object. The Redirect action is executed with the specified settings.

OTP Needed?

This nested rule set provides a one-time password for a user who sends a request for authorized overriding if the requested web object is located on a host within the corporate domain of McAfee.

<table>
<thead>
<tr>
<th>Nested library rule set – OTP Needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <code>URL.Host matches *mcafee.com* AND Quota.AuthorizedOverride.SessionExceeded&lt;Default&gt;</code> equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the host of the URL sent in a request is located within the corporate domain of McAfee and the time quota for a session that can be continued after an authorized override has been exceeded.

The rule set contains the following rules:

Retrieve OTP context

Always → Continue – Authentication.SendOTP<OTP>

The rule uses an event to send a one-time password to an authenticated user. This way the context information is obtained that is required for authenticating a user through a one-time password that is validated on a McAfee OTP server.
Block request and offer sending OTP

*Always* => Block<OTP Required with Pledge>

The rule blocks a request for web access.

The action settings specify that a message is sent to inform the user web access can be allowed after submitting a one-time password that can be obtained from a McAfee Pledge device.

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 is 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:

   \[URL.Port \text{ equals} \ 444 \text{ or } Proxy.Port \text{ equals} \ 444.\]

   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, select 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.
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.

Make sure the Trusted checkbox is selected.

[Optional] In the Comment field, type a plain-text comment on the certificate authority.

Click OK.

The window closes and the certificate authority appears in the list.

Click OK to close the Edit Settings window.

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.

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, select 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.
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.

To configure a different listener port, type the number of this port here.

Click OK to close the Edit Settings window.

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 304
  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 305
  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.

On the wizard pages, proceed as follows:

- On the Welcome page, click Next.
- On the File to Import page, click Browse and navigate to the location where you stored the certificate file.
- In the File Name field, type *.pfx, then press Enter.
- Select the certificate file and click Open, then click Next.
- On the Password page, type a password in the Password field. Then click Next.
- On the Certificate Store page, click Place all certificates in the following store.
- In the Certificate Store section on the same page, select Personal, then click Next.
- On the Completing the Certificate Import Wizard page, click Finish.

Confirm the message that appears by clicking OK.

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.

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.

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.
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.

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.
   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.
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
- Time quota
- Volume quota
- Coaching
- Authorized override
- Blocking sessions

**Imposing quotas and other restrictions on web usage**

Imposing quotas and other restrictions in a quota management process for the users of your network allows you to guide their web usage and limit their consumption of network resources.

The quota management process includes several elements, which contribute to it in different ways.

- Quota management rules control the process.
- Quota management lists 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 by the rules, handle time and volume quotas, session times, and other restrictions within the process.
A quota management process is not implemented by default on Web Gateway after the initial setup. You can implement a process by importing suitable rule sets from the rule set library and modify this process to adapt it to the requirements of your web security policy.

To configure quota management, you can work with:

- **Key elements of rules** — After importing the library rule sets for quota management and clicking them on the rule sets tree, you can view and configure key elements of the rules for the quota management process.
- **Complete rules** — After clicking Unlock View in the key elements view, you can view the rules for the quota management process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

**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**.
**Time Quota rule set**

The Time Quota rule set is a library rule set for imposing time quotas on web usage.

<table>
<thead>
<tr>
<th>Library rule set – Time Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Time Quota With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Time Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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 lsActivationRequest equals true* \(\rightarrow\) *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* \(\rightarrow\) *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* \(\rightarrow\) *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.

<table>
<thead>
<tr>
<th>Nested library rule set – Time Quota With IP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Client.IP is in list IP Blocklist for Time Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Time Quota With Authenticated User Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authenticated.RawUserName is in list User Blocklist for Time Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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**.

**Volume Quota rule set**
The Volume Quota rule set is a library rule set for imposing volume quotas on web usage.

<table>
<thead>
<tr>
<th>Library rule set – Volume Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – SSL.Client.Context.IsApplied equals true OR Command.Name does not equal “CONNECT”</td>
</tr>
<tr>
<td><strong>Cycle</strong> – Requests (and IM)</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Library rule set – Volume Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Volume Quota With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Volume Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Client.IP is in list IP Blocklist for Volume Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Authenticated.RawUserName is in list User Blocklist for Volume Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>MediaType.FromFileExtension at least one n list Media Type Blocklist for Volume Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>
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.
**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.

<table>
<thead>
<tr>
<th>Library rule set – Coaching</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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
  - This rule set is not enabled initially.
- 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.

<table>
<thead>
<tr>
<th>Nested library rule set – Coaching With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Coaching</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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**.

   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**.

**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 an authorized user.

<table>
<thead>
<tr>
<th>Library rule set – Authorized Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.
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**

\[
\text{Quota.AuthorizedOverride.IsActivationRequest<URL Category Configuration> equals true AND}
\text{Authentication.Authenticate<User Database> equals true} \rightarrow \text{Redirect<Redirection After Authorized Session Activation>}
\]

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**

\[
\text{Quota.AuthorizedOverride.SessionExceeded<URL Category Configuration> equals true} \rightarrow \text{Block<Action Authorized Override Blocked>}
\]

The rule uses the \( \text{Quota.AuthorizedOverride.SessionExceeded} \) 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 \( \text{URL Category Configuration} \) 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.

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 \( \text{IP Configuration} \).

**Authorized Override With Authenticated User Configuration**

This nested rule set handles authorized overriding related to user names.

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 \( \text{Authenticated User Configuration} \).
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

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.

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.

<table>
<thead>
<tr>
<th>Library rule set – Blocking Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Blocking Sessions With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Blocking Sessions</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

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 Sessions -- 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.
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
- Edit the text of a user message
- Modifying a block page

## 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.
Different versions can exist of a particular template regarding:

- **Language** — English and other languages
- **File format** — html or txt

Activities that you can complete when editing a message template include 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)

### 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 `$List.Of<String,ByName(String)$`.

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 `NumberTo_String(String)` property.

### Template Editor

The Template Editor is a component of the user interface that allows you to work with templates for messages to users. You can access it in several ways.

- Select it under the **Policy** top-level menu.
- Select the settings for an action:
  - Under **Policy | Settings**
    - OR
  - In a rule of a rule set, after enabling the complete rules view and **Show details**.

Then click **Edit** within these settings for a template collection or an individual template.
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 that **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 configuration 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 **OK** to close the **Edit Settings** window.
11. Click **Save Changes**.

Modifying a block page

You can modify a block page to adapt it to your corporate design and to provide additional information, for example, for debugging purposes.

A block page appears on a client of a Web Gateway when a request for web access is blocked. Use the Template Editor to modify what the user sees on this page.

Other pages sent to users can be modified in the same way as block pages.
Modifying the parts of a block page

A block page consists of header and footer with general information and the middle with issue-related information. These parts should be modified in different ways.

Unlike the issue-related information, header and footer information is shown on all block pages, for example, the corporate logo.

Information on a block page is in many cases provided by inserting suitable properties in the page template. For example, to show the media type of a web object, the `MediaTypeEnsuredTypes` property is inserted, displaying the particular value that applies to a request.

Retrieving a value for a property requires considerable effort in some cases, for example, when Web Gateway must perform a database lookup to retrieve a value, such as the one for `Authentication.Username`. Other properties, for example, `Client.IP` requires less effort.

**Best practice:** Do not insert properties requiring a larger effort to retrieve their values in the header or footer of a block page to avoid an unnecessary impact on performance.

Modify the footer of a block page

Modify the footer of a block page by inserting additional information for debugging purposes.

Inserting the following properties in the footer of a template for a block page provides useful debugging information. The effort for retrieving the values of these properties is rather small.

- `System.Hostname` — Host name of the Web Gateway appliance that handled a request for web access
- `Proxy.IP` — IP address of the Web Gateway appliance that acted as a proxy to handle the request
- `Client.IP` — IP address of the Web Gateway client that the request was sent from
- `Rules.CurrentRule.Name` — Name of the rule that was applied when the request was handled
- `Rules.CurrentRuleSet.Name` — Name of the rule set that the rule belongs to

**Task**

1. Select Policy | Templates.
2. In the Templates pane, expand Default Scheme, then expand the language folder that you want to work with, for example, `en`.
3. Click html.
   
   In the File System pane, the `index.htm` file of the en language folder within the default folder is selected. The content of this file is displayed in the HTML Editor pane.
4. Locate this section of the file content:

```html
<tr>
  <td class='footData'>
    generated at <span id="time">$DateTime.ToISOString$/</span> by McAfee Web Gateway
    <br />
    $Get.Header$
  </td>
</tr>
```
5  Replace this section with the following:

```html
<tr>
  <td class='footData'>
    generated at $<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.datetimefilter.datetime.toISOString"/>$
    by $<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.hostname"/>$
    ($<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.ip"/>$)
    <br />
    Client IP Address: $<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.client.ip"/>$
    <br />
    Rule Name: $<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.rules.currentrulename"/>$
    ($<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.rules.currentrulesetname"/>$)
  </td>
</tr>
```

After replacing the section, the terms representing properties are converted to display the property names. The result should look like this:

```html
<tr>
  <td class='footData'>
    generated at $DateTime.ToISOString$ by $System.Hostname$ ($Proxy.IP$)
    <br />
    Client IP Address: $Client.IP$
    <br />
    Rule Name: $Rules.CurrentRuleName$ ($Rules.CurrentRuleSetName$)
  </td>
</tr>
```

In the footer of a real block page, the current property values will be shown, for example, as follows:

```html
<tr>
  <td class='footData'>
    generated at 2016-09-30 by testhost (10.120.233.2)
    <br />
    Client IP Address: 10.120.233.10
    <br />
    Rule Name: Allow URLs that match in URL WhiteList (URL Filtering)
  </td>
</tr>
```

6  Click Save Changes.

Modify the issue-related part of a block page

Insert additional information in the issue-related part of a block page.

The additional information can, for example, be information about a user who sent a request for web access and has successfully passed the authentication process.

The Authentication.Username property must be inserted in the block page to provide this information. Retrieving a value for this property requires a lookup, but the effort can still be considered as reasonable, as his lookup is not performed each time a block page is displayed.

Task

1  Select Policy | Templates.

2  In the Templates pane, expand Default Scheme, then expand the template and language folders that you want to work with, for example, URL.Blocked, and then en.
3 Click html.

In the File System pane, the URLBlocked.htm file of the en language folder within the default folder is selected. The content of this file is displayed in the HTML Editor pane.

4 Locate this section of the file content:

```
<tr>
  <td class='infoData'>
    <b>URL</b><script type="text/javascript">break_line("$URL$"'></script><br />
    <script type="text/javascript">writeToDocument("<b>URL Categories: </b>" +
    "$Categorylist.ToString"></script><br />
    <b>Reputation</b>: $URLReputationString$<br />
    <b>Media Type</b>: $MediaType.EnsuredTypes$<br />
  </td>
</tr>
```

5 Copy the following line and paste it below the original line.

```
<b>Media Type</b>: $MediaType.EnsuredTypes$<br />
```

6 Replace the words Media Type by User in the pasted line.

7 Delete the property name in this line and place the cursor inside the area that is now empty, then click Add.

8 In the Choose Property window that opens, select Authentication.Username and click OK.

   The property is inserted in the line. Its current value will now be shown when the block page is displayed.

9 Click Save Changes.

**Change the logo on a block page**

Replace the default logo file with a file of your own to change the logo on a block page.

**Task**

1 Store an image file with your logo in a location of your file system.

2 Navigate to the default image file.
   a Select Policy | Templates.
   b In the File System pane, expand default, and then img.
      All image files that are stored in the file system appear.

3 Replace the default image file with your file.
   a Copy the file named mwg_logo.png and rename it to mwg_logo.png-bak.
   b Close the img folder, select the closed folder, and click Add.
c From the menu that opens, select **Existing file or directory**, then select your image file in the file system window that opens and click **Open**.

The file appears in the **img** folder.

d Rename the file to **mwg_logo.png**.

You can give the file a different name, but then you must also replace the default name in the following line of the **index.html** file in the **default** folder with the new name.

```html
<img src='$Proxy.EndUserURL$/files/default/img/logo_mwg.png'>
```

4 Click **Save Changes**.

**Change the color of the background bars on a block page**

Replace the default image file for the background bars with a file of your own to change the color of those bars.

**Task**

1 Store an image file with background bars of your preferred color in a location of your file system.

2 Navigate to the default image file.
   a Select **Policy | Templates**.
   
   b In the **File System** pane, expand **default**, and then **img**.

   All image files that are stored in the file system appear.

3 Replace the default image file with your file.
   a Copy the file named **bg_navbar.png** and rename it to **bg_navbar.png-bak**.
   
   b Close the **img** folder, select the closed folder, and click **Add**.
   
   c From the menu that opens, select **Existing file or directory**, then select your image file in the file system window that opens and click **Open**.

   The file appears in the **img** folder.
   
   d Rename the file to **bg_navbar.png**.

You can give the file a different name, but then you must also replace the default name in the following line of the **index.html** file in the **default** folder with the new name.

```html
<td class='helpDeskData' background='$Proxy.EndUserURL$/files/$Proxy.Message.Collection$/img/bg_navbar.jpg'>
```

4 Click **Save Changes**.

You can change more colors by modifying the **stylesheet.ccs** file in the **default** folder.

For example, by replacing the color code in the following line, you can modify the general background color of the template.

```css
body {
    background-color: #ced1d4;
}
```
User messages
Modifying a block page

...
Supporting functions

Web Gateway also provides functions, such as web caching or progress indication that do not themselves filter web objects, but support the filtering process in different ways.

Contents
- Functions supporting web filtering
- Web caching
- Progress indication
- File opening
- Bandwidth throttling
- Next-hop proxies

Functions supporting web filtering

Some of the functions that support web filtering are implemented by rule sets of the default rule set systems. Rule sets for other functions can be imported from the library.

The default rule sets for supporting functions are all embedded in the Common Rules rule set. Rule sets for web caching, progress indication, use of file openers, and other functions can be found here.

The library provides rule sets for bandwidth throttling and the use of next-hop proxies for web access.

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. The Enable.Cache event is used in these rules for enabling the web cache.

Additionally, there can be bypass rules that exclude objects from being read or written.

You can configure the Cache HTTP module settings to modify the caching behavior, for example, if you want to increase the caching rate.
Cache settings

You can configure the Cache HTTP module settings to modify the caching behavior, for example, if you want to increase the caching rate. These settings are provided with the Enable.Cache event.

Modifying the caching behavior can, however, lead to unfavorable results, for example, if requests that include web server authentication or responses with a Vary header are cached.

We therefore recommend using a default rule with the Always criteria and additional rules that enable web caching depending on more specific criteria. For example, the criteria might use the URL.Host property to specify a particular host.

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.

Web Cache rule set

The Web Cache rule set is a library rule set for web caching.

<table>
<thead>
<tr>
<th>Library rule set – Web Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM) and responses</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Read from Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested library rule set – Write to Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
<tr>
<td>Cycles – Responses</td>
</tr>
</tbody>
</table>

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.
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.
Best practice: Working with progress indication methods

To provide progress indication for a user who requested a file upload or download, you can work with suitable progress indication methods according to your working environment.

The following methods are available:

• **Progress pages** — Progress pages keep the user informed about downloading and scanning times and provide a link for obtaining the completely processed file.

  We recommend using progress pages as the default method. Apply other methods only if progress pages are not eligible, for example, when the web browser used for downloading is not Mozilla-compatible.

  When the default Progress Indication rule set is implemented, use of progress indication methods follows this recommendation.

• **Data trickling** — Data trickling informs the user about the estimated overall processing time without indicating the portion that is required for anti-malware scanning.

  This method can, however, be used for any kind of download regardless of the web browser type.

• **FTP upload timeout prevention** — This method can only be used for uploading files when Web Gateway is configured to run as an FTP proxy.

  The upload is not performed using a web browser, but requires a standalone FTP client, which can be implemented, for example, using Filezilla.

Working with progress pages

You can use progress pages with web browsers that are Mozilla-compatible. Taking packet captures allows you to track the progress indication workflow and detect issues.

Mozilla-compatible browsers

Progress pages only work for web browsers that announce their compatibility with Mozilla in the User-Agent headers of HTTP requests. This includes, for example, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, and Safari, but not Opera.

A packet capture of an HTTP request created, for example, using Wireshark, shows whether your browser is Mozilla-compatible. The capture contains a line about the User-Agent, such as the following:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
```

This line shows that your browser is Microsoft Internet Explorer (MSIE) and that it is indeed Mozilla-compatible. For other browsers, the User-Agent lines might look as follows.

Firefox:

```
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:23.0) Gecko/20100101 Firefox/23.0
```

Chrome:

```
User-Agent: Mozilla/5.0 (Windows NT 5.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.57 Safari/537.36
```
Workflow for progress pages

When progress pages are enabled on Web Gateway, a page showing the download and scanning progress is provided, as well as a page that announces download completion and offers a link for obtaining the fully downloaded file.

By creating packet captures with, for example, Wireshark, you can track the workflow as needed to detect issues. In the following example, three devices with the following IP addresses appear in the workflow:

- A client of Web Gateway: 10.10.80.1
- Web Gateway: 10.10.80.57
- A web server: 10.10.80.200

The workflow includes the following main steps.

1. A client sends a request for downloading a large file from a web server.

   ![Message capture]

2. Web Gateway redirects the client to the progress page, sending the following HTTP status: 307 Moved Temporarily.

   The redirection specifies a location with the same IP address as in the request that was originally sent by the client, but with the subdirectory information changed to enable redirection to the progress page.

   ![Location capture]

3. The client opens a new TCP connection to Web Gateway, sends a request for the location that it was redirected to, and starts downloading the progress page.

   The download begins with a message that contains the following request.

   ![Request capture]

Due to the mwg-internal subdirectory information in the request, Web Gateway knows that the requested page is locally available. It provides this page to the client, rather than querying the web server that is identified by the IP address in the request.
4 After downloading the progress page, the client requests an update from Web Gateway every five seconds, for example, as follows.

```
GET http://10.10.80.200/mwg-internal/de5fs23hu73ds/progress?id=29qNbsp9oR&a=1&1377106154955 HTTP/1.1
```

5 Web Gateway responds according to the progress made, sending the following HTTP status: 200 OK. With this status, line-based text data is sent to indicate the progress.

The text data includes five values with particular meanings.

- For example, in the following response, the text data indicates that Web Gateway has started downloading the requested file.

```
16.3 MB; 204.5 MB; 7; 0; 0
```

The meaning of each value in this response is as follows.

- 1 – Amount of data downloaded so far from web server
- 2 – Total amount of data to be downloaded
- 3 – Percentage of download completion
- 4 – Anti-malware scanning complete? (0 = No, 1 = Yes)
- 5 – Time (in seconds) consumed so far by anti-malware scanning

So, here the text data indicates that Web Gateway has already downloaded 16.3 MB from a file that is 204.5 MB large, which amounts to 7 percent, and that anti-malware scanning has not started yet.

- In this response, the text data indicates that Web Gateway has downloaded the file and started anti-malware scanning, which is not yet complete.

```
204.5 MB; 204.5 MB; 100; 0; 153
```

- In this response, the text data finally indicates that Web Gateway has completed anti-malware scanning.

```
204.5 MB; 204.5 MB; 100; 1; 4512
```

The web browser now presents the user with a link for downloading the requested file to the client.

**Workflow for data trickling**

When data trickling is enabled, Web Gateway downloads a requested file and sends tiny pieces of it to the requesting client. This keeps the connection alive while Web Gateway downloads the whole file and scans it for infections. This means that while the scanning process is going on, the data moves at a very slow rate.

If Web Gateway detected an infection after the file had been completely downloaded, only a small amount of the file would have been passed on. So the client would not have received enough malicious data to let any harm be caused.
In more detail, the workflow for data trickling is as follows.

1. Web Gateway sends an initial chunk, which is 4,096 bytes long, followed by 1 byte for every 1,000 that are downloaded, as long as the file is scanned for infections.

   As estimations of the download time are provided by the web browser, which is not aware of any Web Gateway activities, estimated download times look extremely long to the user at the beginning.

   For example, about 58 hours are estimated for downloading a 204 MB file, as shown in the following lines within the web browser.

   ```
   big_archive.zip from 10.10.80.200
   Estimated time left 58 hr 10 min (4.80 KB of 204 MB copied)
   Download to: C:\Documents and Settings\big_archive.zip
   ```

2. When Web Gateway has finished anti-malware scanning and found no infections, it sends the remaining portion of the file to the client at full network speed.

**Workflow for FTP upload timeout prevention**

When FTP upload timeout prevention is enabled, Web Gateway sends progress indication messages to the FTP client that sent a file for uploading to an FTP server.

The messages are sent every five seconds. This keeps the TCP connection alive and gives Web Gateway time to scan the file for infections.

The messages can be viewed on the FTP server using, for example, the Filezilla tool that was also used to install the FTP client.

In more detail, the workflow for FTP upload timeout prevention is as follows.

1. Web Gateway uploads a file from the client and starts anti-malware scanning. While the scanning is in progress, Web Gateway sends a progress indication message to the client every five seconds.

   ```
   Response: 150 File status OK; about to open data connection.
   Response: 226-data processing in progress
   Response: 226-data processing in progress
   ...
   ```

   When the file has been uploaded to Web Gateway, this is indicated by a completion message.

   ```
   C:\Documents and Settings ... --> /home admin small_archive.zip  876,241
   Normal  Transferring
   00:00:00 elapsed  -:-:-left  100%  876,241 bytes
   ```

   The file is not yet visible, however, on the FTP server.

2. After Web Gateway has finished anti-malware scanning and found no infection, it uploads the file to the FTP server and sends a status message to the FTP client.

   ```
   ...
   Response: 226-data processing in progress
   Response: 226-data processing in progress
   Response: 226 File receive OK
   Status: File transfer successful, transferred 876,241 bytes in 26 seconds
   ```

   The file is now visible on the FTP server.
**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.

<table>
<thead>
<tr>
<th>Library rule set – Progress Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – MediaType.FromHeader does not equal text/html</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

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 html type.

The rule set contains the following rules.

**Enable progress page**

`Header.Request.Get ("User-Agent") matches regex (*.mozilla.*)` → 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.

**FTP upload timeout prevention**


The rule enables the FTP Upload Progress Indication function if a file has been sent from a client for uploading to the web under the FTP protocol.

Messages indicating upload progress are then sent to the client during the upload to prevent a timeout that could occur on the client if the upload takes more time.

This could be due, for example, to scanning the file that is to be uploaded for infections by viruses and other malware.

**Enable 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.

**File opening**

File opening is performed on Web Gateway to make files available for inspection and filtering that cannot immediately be accessed, for example, because they are nested in an archive or have been encrypted or compressed.

File opening is handled by a Web Gateway component that is known as the Composite Opener. This opener is capable of opening archives and encrypted or compressed files in various formats. Its use is controlled by rules.

**File opening process**

File opening is performed by an opening component on Web Gateway and controlled by rules.

The Composite Opener, which performs the file opening is enabled by a rule in a default rule set. The rule itself is by default enabled.

Other rules are provided in this rule set, which can be enabled to block files that have been recognized as archives or as encrypted or corrupted files.

The name of the default rule set that contains these rules is **Enable Opener**. It is a nested rule set of the default **Common Rules** rule set.
The **Composite Opener** settings can be configured to set a limit to the number of levels that nesting can include within an archive. When this limit is exceeded, no file opening is performed.

**Formats for file opening**

File opening is performed on Web Gateway by the Composite Opener, which can handle various formats of files that are archives or encrypted or compressed files.

The formats that can be handled include, for example, the following.

- application/vnd.ms-windows-imaging-file format
- gzip default encoding format
- Brotli encoding format
- rpm archive format
- DMG file format

**Enable Opener rule set**

The **Enable Opener** rule set is the default rule set for handling file opening on Web Gateway.

**Key elements of the Enable Opener rule set**

The key elements of the **Enable Opener** rule set include settings for file opening and several block options.

**Table 14-1  Key elements of the Enable Opener rule set**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Composite Opener settings</td>
<td>Clicking <strong>Edit</strong> makes the Composite Opener settings available for editing.</td>
</tr>
<tr>
<td>Block encrypted media types</td>
<td>When selected, a rule is enabled that blocks encrypted media types.</td>
</tr>
<tr>
<td>Block multipart media types</td>
<td>When selected, a rule is enabled that blocks multipart media types.</td>
</tr>
<tr>
<td>Block corrupted media types</td>
<td>When selected, a rule is enabled that blocks corrupted media types.</td>
</tr>
</tbody>
</table>

**Complete rules of the Enable Opener rule set**

The **Enable Opener** rule set includes the following rules.

**Default rule set – Enable Opener**

- **Criteria** – **Always**
- **Cycles** – Requests (and IM), Responses, Embedded Objects

**Enable Composite Opener**

- **Always** -> Continue – Enable Composite Opener <Default>

The rule uses the **Enable Composite Opener** event to enable the Composite Opener on Web Gateway for file opening.

The opener is enabled with the **Default** settings.

**Block encrypted media types**

- **Body.IsEncryptedObject equals true** -> Block<Not Supported Archive>

The rule uses the **Body.IsEncryptedObject** property to check whether a requested media type is encrypted.

If it is, the request is blocked and not passed on to the requested web server.

The event settings specify a message to the requesting user.
Block multipart media types

Body.IsMultiPartObject equals true --> Block<Multipart Archive>

The rule uses the Body.IsMultiPartObject property to check whether a requested media type is a multipart object.

If it is, the request is blocked and not passed on to the requested web server.

The event settings specify a message to the requesting user.

Block corrupt media types

Body.IsCorruptedObject equals true --> Block<Media Type (Common)>

The rule uses the Body.IsMultiPartObject property to check whether a requested media type is a multipart object.

If it is, the request is blocked and not passed on to the requested web server.

The event settings specify a message to the requesting user.

Bandwidth throttling

You can limit the speed for uploading and downloading data to the appliance in a process known as bandwidth throttling.

Bandwidth throttling is also known as bandwidth control.

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 uploading objects to the web or are requesting large downloads from the web.
Two methods of bandwidth throttling are available on Web Gateway.

- **Basic bandwidth throttling** — Using this method you can limit the speed of data transfer from a client to a Web Gateway appliance and from the appliance to a web server.

  Under this method, you configure suitable rules that specify a maximum transferring speed. When an upload or download request matches the criteria of a rule, the speed of transferring data for this request is limited as specified in the rule.

- **Bandwidth throttling using classes** — Using this method you can limit the speed of data transfer from a client to a Web Gateway appliance and from the appliance back to the client, as well as from an appliance to a web server and from the web server back to the appliance.

  Under this method, you configure classes of transferring speed and suitable rules that make use of them. A class is specified by a speed range, for example, 1001 to 2000 Kbps.

  When an upload or download request matches the criteria of a rule, the speed of transferring data for this request is limited as specified by the class used in the rule. This speed must not exceed the maximum value, nor fall below the minimum.

  You can, for example, create a rule that applies to downloads of Windows updates and prevents them from consuming all of the bandwidth that is available on your system by limiting it to the transferring speed range of a particular class.

  You can also limit the speed of data transfer performed for traffic that does not use the proxy functions of Web Gateway, which means that the rules of your web security policy are not applicable.

  This traffic originates, for example, when Web Gateway log files are uploaded to an external server or data is downloaded from an external server to update information required for performing filtering functions on Web Gateway.

### Basic bandwidth throttling

Basic bandwidth throttling limits 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.

### Bandwidth 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.

**Bandwidth 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**

\[
\text{MediaType.EnsuredTypes at least one in list MediaType Throttling List} \rightarrow \text{Continue} \rightarrow \text{Throttle.Server (1000)}
\]

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
Create a rule set for bandwidth throttling.

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.

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.

Save your changes.

**Bandwidth throttling using classes**

Bandwidth throttling can be performed on Web Gateway using classes, which cover ranges of data transferring speed.

Bandwidth throttling is also known as *bandwidth control*.

A bandwidth class can, for example, cover the speed range between 1 and 1000 Kbps, while another class covers 1001 to 2000 Kbps. Using an event in a rule, you can configure that particular web objects are uploaded or downloaded with the speed of either of these two classes or any other class that you have created.

You can also group classes and subordinate them to parent classes, assigning different priorities to the classes in a group.

Bandwidth throttling using classes can be configured for all directions that web traffic flows into. The speed of downloads requested by clients of Web Gateway can be throttled, as well as the speed of uploads.

This throttling method can be used for throttling transferring speed, but also for ensuring a minimum speed when web objects are uploaded or downloaded. In most cases, however, its main purpose will be limiting the speed of voluminous downloads from the web.

Bandwidth throttling using classes is available for most of the different network modes that can be configured for the proxy functions of Web Gateway. These modes include the explicit proxy mode, the proxy HA mode, and the transparent modes.

Bandwidth throttling using classes can also be applied to traffic that is not using the proxy functions of Web Gateway.

**Events in rules for bandwidth throttling using classes**

The following events are available for use in rules that control bandwidth throttling using classes:

- **Bandwidth.FromClient** — Limits the speed of data transfer from a client to the appliance
- **Bandwidth.ToServer** — Limits the speed of data transfer from the appliance to a web server
- **Bandwidth.FromServer** — Limits the speed of data transfer from a web server to an appliance
- **Bandwidth.ToClient** — Limits the speed of data transfer from the appliance to a client
When these events are used in rules, they take the name of a bandwidth class as a parameter. This way traffic can be throttled in any direction according to the limits that are configured for the respective class.

**Bandwidth throttling rule for downloads**

The following is an example of a bandwidth throttling rule. It applies bandwidth throttling using classes to downloads of large files from the web.

<table>
<thead>
<tr>
<th>Name</th>
<th>Limit transferring speed for large downloads</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Body.Size greater than 1000000&quot;</td>
<td>---&gt;</td>
<td>Continue Bandwidth.FromServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(&quot;Large&quot;)</td>
</tr>
</tbody>
</table>

The rule uses the `Bandwidth.FromServer` event to limit the speed at which downloads from a web server are performed.

If the size of a web object that is sent as the body of a response from the server exceeds 10 MB, the transferring speed is limited to a particular speed range. This speed range is the range that you configured for the bandwidth class named `Large`, for example, between 1 and 1000 Kbps.

**Configure bandwidth throttling using classes**

To configure bandwidth throttling using classes, create bandwidth classes and suitable rules that use these classes.

**Task**

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance that you want to configure bandwidth throttling on, then click Bandwidth Control.
   
   The Bandwidth Control settings appear in the configuration pane.
3. Under Bandwidth Control, make sure that Enable Bandwidth Control is selected.
   
   Make sure that any other bandwidth throttling functions on Web Gateway are disabled.
4. Under Bandwidth Classes, configure the classes that you want to use for bandwidth throttling.
   a. In the Bandwidth classes list, add entries for bandwidth classes.
   b. In the Interface names list, add entries for the network interfaces on Web Gateway that bandwidth throttling using classes are performed on.
5. Create suitable rules that use the bandwidth throttling events and classes to limit the transferring speed of data in incoming and outgoing web traffic on Web Gateway.
   
   When creating a rule, make sure that you only reference classes at the lowest hierarchy level, as only the speed limits configured for these classes are applied to data transfers.

**Configuring bandwidth throttling for non-proxy traffic**

You can apply bandwidth throttling to limit the speed of data transfer that is not using the proxy functions of Web Gateway.

This kind of traffic originates, for example, when Web Gateway log files are uploaded to an external server or data is downloaded from an external server to update information required for performing filtering functions on Web Gateway.
As the usual web security rules are not applicable to this traffic, specific rules, which are static, must be configured here for bandwidth throttling.

**Configuring bandwidth throttling for different network modes**

Bandwidth throttling using classes can be configured for most of the different network modes that Web Gateway can run in as a proxy.

These modes include:

- Explicit proxy
- Transparent proxy using WCCP
- Proxy HA
- Transparent router
- Transparent bridge

When configuring bandwidth throttling using classes for any of these modes, you specify bandwidth classes and the network interfaces for the web traffic that these classes are used on.

For the proxy HA mode and the transparent router and bridge modes, the configuration of network interfaces differs depending on whether you want to configure a particular Web Gateway appliance as a director node or a scanning node.

When configuring a director node, you must specify network interfaces for both incoming and outgoing web traffic. This applies both to configuring an active and a fail-over director node. A scanning node only requires a network interface for outgoing web traffic.

IP spoofing must be disabled in the Proxies settings for the proxy HA mode, the transparent router and bridge modes, as well as for the transparent proxy mode using WCCP.

**Configure bandwidth throttling for the transparent router and bridge modes and the proxy HA mode**

Configure bandwidth throttling using classes for the transparent router and bridge modes, as well as for the proxy HA mode, by creating bandwidth classes and specifying network interfaces depending on whether a Web Gateway acts as a director or scanning node.

IP spoofing must be disabled in the Proxies settings when configuring bandwidth throttling using classes for these network modes.

**Task**

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance that you want to configure bandwidth throttling on, then click Bandwidth Control.

3. Make sure that Enable bandwidth control is selected.

4. In the Bandwidth classes list under Bandwidth Classes, create the bandwidth classes that will be used for bandwidth throttling when running Web Gateway in these network modes.

5. In the Interface names list under Bandwidth Classes, specify the network interfaces for bandwidth throttling.

   - When configuring an appliance as an active or fail-over director node:
     1. Click the Add icon.
     2. In the Add Interfaces Name window that opens, select the name of a network interface name for inbound web traffic, for example, eth0, then click OK.
3 In the same window, select the name of a network interface name for outbound web traffic, for example, eth1, and click OK.

4 Click Save Changes.

• When configuring an appliance as a scanning node:
  1 Click the Add icon.
  2 In the Add Interfaces Name window that opens, select the name of a network interface name for outbound web traffic, for example, eth1, then click OK.
  3 Click Save Changes.

**Next-hop proxies**

Next-hop proxies can be used as an additional means of forwarding requests received from the clients of an appliance to their destinations.

When next-hop proxies are implemented, a rule in a corresponding rule set uses a module (also known as engine) to call next-hop proxies that have been entered into a list for forwarding requests.

For example, you can forward requests that have internal destinations using internal next-hop proxies. IP addresses of destinations that are internal are then entered into a list, which the forwarding rule relies on. In addition to this, there is a list of internal next-hop proxies for use by the rule.

A rule set with a rule 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 the next-hop proxy rule set, a list of servers that can be used as next-hop proxies is also imported. The list 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 the library rule set. You can configure these settings to let the module use a particular next-hop proxy list and to determine the mode of calling the next-hop 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 several modes to call them: Round-robin, failover, and stickiness.

**Round-robin mode for next-hop proxies**

When routing a request in round-robin mode, the next-hop proxy module calls the next-hop proxy 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.

![Diagram](image1.png)

**Figure 14-1 Next-hop proxies in round-robin mode**
The round-robin mode is configured as part of the settings for next-hop proxies.

**Failover mode for next-hop proxies**
When routing a request in failover mode, the next-hop proxy module calls the first next-hop proxy on the list. If this next-hop proxy fails to respond, the call is repeated until the configured number of retries is reached. Only then is the second next-hop proxy in the list tried. It is called in the same way as the first, and eventually the third next-hop proxy in the list is tried.

This is continued until a next-hop proxy responds or all next-hop proxies in the list were found to be unavailable.

The following diagram shows a next-hop proxy configuration in failover mode.

![Diagram](image2.png)

**Figure 14-2 Next-hop proxies in failover mode**
The failover mode is configured as part of the settings for next-hop proxies.
Next-hop proxy stickiness

A next-hop proxy can also be selected according to what is known as the "sticky" mode. In this mode, requests of a particular kind, for example, requests coming in from the same client of Web Gateway are directed to the same next-hop proxy.

The part of a request that qualifies it for being handled in sticky mode is configured as the value of a property on Web Gateway. An event in a rule sets the property to this value.

The name of the property that is configured to enable next-hop proxy stickiness is `NextHopProxy.StickinessAttribute`. If you want, for example, to let requests from the same client be directed to the same next-hop proxy, you can use the IP address of a client as the value for this property.

In addition to creating a rule, you must also select stickiness as an option within the settings for handling next-hop proxies. The settings also include an option for limiting the time that the next-hop proxy stickiness mode is applied.

Rule for configuring next-hop proxy stickiness

The following sample rule sets the `NextHopProxy.StickinessAttribute` property to the value of the `Client.IP` property to let requests with the same client IP address be directed to the same next-hop proxy.

<table>
<thead>
<tr>
<th>Name</th>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set next-hop proxy stickiness attribute</td>
<td>Always</td>
<td>Continue</td>
<td><code>Set NextHopProxy.StickinessAttribute = IP.ToString(Client.IP)</code></td>
</tr>
</tbody>
</table>

The rule uses an event to set the `NextHopProxy.StickinessAttribute` property. As this property is of the string type, the value for the `Client.IP` property must be converted into a string before it can be used for setting the `NextHopProxy.StickinessAttribute` property.

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.
Add a next-hop proxy to a list
To add a next-hop proxy to a list, complete the following steps.

**Task**

1. Open the Edit Settings window for settings of the Next Hop Proxy module.

2. Under Next Hop Proxy Server, select a next-hop proxy list from List of next-hop proxy servers and click Edit.
   
   The Edit List (Next Hop Proxy Server) window opens.

3. Under List Content, click the Add icon.
   
   The Add Next Hop Proxy window opens.

4. Configure settings for a next-hop proxy as needed.

5. Click OK for all open windows.

6. Click Save Changes.

The next-hop proxy is added to the list that you selected.

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**


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.
Configure next-hop proxy stickiness

To configure next-hop proxy stickiness, select this mode in the Next Hop Proxy settings and add a stickiness rule to a rule set for handling next-hop proxies.

Task

1. Select the stickiness mode for next-hop proxies.
   a. Select Policy | Settings.
   b. On the Engines branch of the settings tree, expand Next Hop Proxy and select the settings that you want to configure next-hop proxy stickiness for.
   c. Under Next Hop Proxy Server select Sticky.
   d. Under Minimum time for stickiness, modify the time period during which the stickiness mode is applied as needed.

2. Add a rule for next-hop proxy stickiness.
   b. Open a rule set for next-hop proxy handling, for example, the Next Hop Proxy library rule set.
   c. Add a rule that sets the NextHopProxy.Stickiness.Attribute property to the value for identifying the requests that are directed to the same proxy.

3. Click Save Changes.

Requests that contain the part specified in the additional rule are now directed to the same next-hop proxy during the configured time period.

Next-hop proxies for SOCKS traffic

A next-hop proxy can be configured to forward web traffic under the SOCKS (Sockets) protocol. Under this protocol, web traffic also follows an embedded protocol, which can be detected on Web Gateway. If the embedded protocol is HTTP or HTTPS, web traffic can be filtered according to the configured rules.

Versions 4 and 5 of the SOCKS protocol can be used for forwarding web traffic. When setting up a next-hop proxy, you can configure the SOCKS version to use. By default, the version of the incoming traffic is also used when it is forwarded.

Configure a next-hop proxy for SOCKS traffic

To configure a next-hop proxy for SOCKS traffic, let Web Gateway run as a SOCKS proxy and implement suitable rule sets for enabling a next-hop proxy and filtering the traffic.

Tasks

• Enable a SOCKS proxy on page 355
  Enable Web Gateway to run as a SOCKS proxy by configuring the proxies settings accordingly.

• Configure a next-hop proxy rule set for SOCKS traffic on page 355
  To configure a rule set for SOCKS traffic, modify the criteria of the Next Hop Proxy library rule set and add a rule that enables a next-hop proxy under the SOCKS protocol.

• Configure the SOCKS Proxy rule set on page 355
  Configure a setting in the SOCKS Proxy rule set that is required for filtering traffic that is forwarded to next-hop proxies under the SOCKS protocol.
Enable a SOCKS proxy
Enable Web Gateway to run as a SOCKS proxy by configuring the proxies settings accordingly.

**Task**
1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the Web Gateway appliance that you want to configure for running as a SOCKS proxy and click **Proxies**.
3. Scroll down to the **SOCKS Proxy** section and select **Enable SOCKS proxy**.
4. Click **Save Changes**.

**Configure a next-hop proxy rule set for SOCKS traffic**
To configure a rule set for SOCKS traffic, modify the criteria of the Next Hop Proxy library rule set and add a rule that enables a next-hop proxy under the SOCKS protocol.

**Task**
1. Import the **Next Hop Proxy** library rule set from the library.
2. On the rule sets tree, move the rule set up and let it follow immediately after the rule set that you are using for authenticating users, for example, the **Explicit Proxy Authentication and Authorization** rule set.
3. Replace **Always** as the rule set criteria by **Connection.Protocol equals "SOCKS"**.
4. Add a rule that enables a next-hop proxy.
   a. Configure the rule criteria to let the rule apply for particular requests.
      For example, use **Client.IP matches in list Client IP** as the rule criteria to let the rule apply only for requests sent from clients with an IP address that is on a particular list.
   b. Configure Continue as the rule action.
   c. Configure Enable Next Hop Proxy as the rule event.
   d. Configure the settings of the rule event.
      • Add a next-hop proxy to the list of next-hop proxies.
      When adding the next-hop proxy, make sure that you specify the SOCKS parameters as needed.
      • Configure the remaining options as needed.
5. Click **Save Changes**.

You can add more rules to the Next Hop Proxy rule set, using different criteria each time for setting up a next-hop proxy.

**Configure the SOCKS Proxy rule set**
Configure a setting in the SOCKS Proxy rule set that is required for filtering traffic that is forwarded to next-hop proxies under the SOCKS protocol.

**Task**
1. Import the **SOCKS Proxy** rule set from the library.
   The rule set can be found under **Common Rules**.
2. On the rule sets tree, let the rule set follow immediately after the **Next Hop Proxy** rule set.
3 In the nested Protocol Detection rule set of the SOCKS Proxy rule set, click the settings for the Protocol Detector module.

   The default name of these settings is Default.

   The Edit Settings window opens.

4 Under Protocol Detector Options, select Determine next-hop proxy after receiving embedded data.

5 Click OK to close the window.

6 Click Save Changes.

For more information about the SOCKS Proxy rule set, see the Proxies chapter.

Rules for enabling next-hop proxies for SOCKS traffic

You can add various rules to the Next Hop Proxy rule set, using different criteria for setting up a next-hop proxy.

The following rule enables a next-hop proxy for a request that was received from a client of Web Gateway with an IP address that is on a particular list.

Name

Enable next-hop proxy for SOCKS traffic if received from listed client

Criteria Action

Client.IP matches in list Client IPs

   -- > Continue  Enable Next Hop Proxy<SOCKS Next Hop Proxy>

The rule uses the Client.IP property to check whether the IP address of the client that a request was received from is on the list.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

The next rule enables a next-hop proxy if the embedded protocol under the SOCKS protocol is HTTP.

Name

Enable next-hop proxy for SOCKS traffic with embedded HTTP protocol

Criteria Action

ProtocolDetector.DetectedProtocol<Default> equals "HTTP"  -- > Continue  Enable Next Hop Proxy<Embedded Protocol HTTP Next Hop Proxy>

The rule uses the ProtocolDetector.DetectedProtocol< property to check whether the embedded protocol is HTTP.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

When using this rule, you also need to enable the option Determine next-hop proxy after receiving embedded data in the settings for the Protocol Detector module (or engine).

The next rule enables a next-hop proxy if the embedded protocol under the SOCKS protocol is HTTPS.

Name

Enable next-hop proxy for SOCKS traffic with embedded HTTPS protocol

Criteria Action

ProtocolDetector.DetectedProtocol<Default> equals "HTTPS"  -- > Continue  Enable Next Hop Proxy<Embedded Protocol HTTPS Next Hop Proxy>
The rule uses the `ProtocolDetector.DetectedProtocol` property to check whether the embedded protocol is HTTP. In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

When using this rule, you also need to enable the option **Determine next-hop proxy after receiving embedded data** in the settings for the Protocol Detector module (or engine).

The next rule enables a next-hop proxy for any embedded protocol under the SOCKS protocol.

**Name**

**Enable next-hop proxy for SOCKS traffic with any embedded protocol**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
</table>

The rule uses the `Connection.Protocol.Parent` property to check whether the SOCKS protocol appears as the parent protocol in a request for forwarding SOCKS traffic to the web. If SOCKS appears as the parent protocol, it means that there must be an embedded protocol.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

The next rule is very similar to the preceding rule. It enables a next-hop proxy for traffic under the SOCKS protocol or traffic that goes on under the HTTP protocol directly, without being embedded in the SOCKS protocol.

**Name**

**Enable next-hop proxy for SOCKS traffic with any embedded protocol**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
</table>

**Best practices - Troubleshooting next-hop proxy issues**

Reviewing the settings for next-hop proxies can help solve issues with connection delays or unavailability. Next-hop proxy issues are indicated by alerts on the dashboard. Settings for next-hop proxies can be reviewed to troubleshoot these issues and also to ensure that next-hop proxies have appropriately been configured to enable cloud lookups for URL filtering and regular updates of other filtering information.
**Next-hop proxy alerts**

Alerts on the dashboard indicating next-hop proxy issues look like this.

- **Next hop proxy 10.44.44.44 has been marked as down for 10 seconds**
  
  This alert appears if, after trying to connect to a next-hop proxy, Web Gateway detects that the next-hop proxy is down and 10 seconds are configured as the waiting time until the next retry.

  The waiting time begins after the configured number of retries, which are performed immediately, have been completed unsuccessfully.

- **Connection to next hop proxy 10.44.44.44 failed**
  
  This alert appears, if after trying to connect to a next-hop proxy, Web Gateway detects that the next-hop proxy is down and no waiting time (0 seconds) is configured. After unsuccessfully completing the configured number of retries, Web Gateway immediately performs the next retry.

**Connection retry settings for next-hop proxies**

If you notice slowness on next-hop proxy connections, we recommend reviewing the connection retry settings, which are part of the **Next Hop Proxy** settings.

The settings include the number of retries Web Gateway performs after a failed connection attempt, and the waiting time before performing the next retry after the configured number of retries has been completed unsuccessfully.

We recommend configuring a low number of retries, for example, 3, and no waiting time at all.

Configuring the settings in this way does not prevent the alerts from appearing, but avoids unnecessary delay with connection retries.

Avoiding delay is also important, as sometimes a next-hop proxy can erroneously be marked as down on Web Gateway, which would make waiting until the next retry even less appropriate.

**Next-hop proxies for URL filtering**

Slowness or failure in URL filtering can also be related to the next-hop proxy configuration.

The settings for URL filtering are by default configured to let categorizations of URLs be looked up on a cloud server of the McAfee Global Threat Intelligence system if no category for a given URL can be found in the local database on a Web Gateway appliance.

Next-hop proxies can be configured for connecting to these servers as part of the **URL Filter** settings. If no next-hop proxies are configured or if the configuration settings are faulty, attempts to perform cloud lookups can fail or be slow.

**Next-hop proxies for updates**

You can also use next-hop proxies for connecting to the update servers, which provide regular updates for anti-malware filtering, URL filtering, and other activities. Next-hop proxies for updates are configured as part of the **Central Management** settings.

**Review the connection retry settings for next-hop proxies**

Review the connection retry settings for next-hop proxies to troubleshoot connection issues.

The connection retry settings can cause additional delay on connections if not appropriately configured.
Task
1 Navigate to the connection retry settings for next-hop proxies.
   a Select Policy | Settings.
   b On the settings tree, expand Next Hop Proxy and click the settings that you want to review.
      The settings appear in the configuration pane.
   c Under Next Hop Proxy Server, select a list of next-hop proxy servers and click Edit.
      The Edit List (NextHopProxy) window opens.
   d From the List Content list, select a next-hop proxy and click Edit.
      The Edit NextHopProxy window opens.
2 Under Next Hop Proxy Definition, configure the following.
   a Set Number of retries to 3.
   b Set After final failure wait to 10 (seconds).
   Close all open windows when you are done.
3 Click Save Changes.

Review the settings of next-hop proxies for URL filtering
Review the settings of next-hop proxies that are used in URL filtering to troubleshoot connection issues. Next-hop proxies are used in URL filtering to connect to the cloud servers of the McAfee Global Threat Intelligence system.

Task
1 Select Policy | Settings.
2 On the settings tree, expand URL Filter and click the particular settings that you want to review.
   The settings appear in the configuration pane.
3 Scroll down to Advanced Settings and check whether one or more next-hop proxies are correctly configured under Proxy Settings.
4 Correct the settings as needed. If no next-hop proxy is configured, add settings for one or more of them.
5 Click Save Changes if you have modified or made additions to the settings.

Review the settings of next-hop proxies for updates
Review the settings of next-hop proxies used for updates to troubleshoot connection issues. Next-hop proxies are used for updates to connect to the various update servers.

Task
1 Select Configuration | Appliances.
2 On the appliances tree, select the appliance that you want to review settings on and click Central Management.
3 Scroll down to **Automatic Engine Updates** and verify that the following applies:
   - **Enable Update Proxies** is selected.
   - One or more next-hop proxies are correctly configured under **Update proxies**.

4 Correct the settings as needed. If no next-hop proxy is configured, add settings for one or more of them.

5 Click **Save Changes** if you have modified or made additions to the settings.

**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 destinations.

<table>
<thead>
<tr>
<th>Library rule set – Next Hop Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Use proxy depending on the destination**

- **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 has been entered into a list directly. If it is, the rule uses an event to forward requests for 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.
Cloud single sign-on (SSO) is the Web Gateway service that allows end users in your organization to access cloud services and applications after providing credentials one time. The SSO service is implemented by the Single Sign On module.

In the context of cloud single sign-on, unless otherwise noted, the following terms are used as described here:

- The term **Service Provider** refers to the organization that provides the cloud service or application.
- The terms **cloud service** and **cloud application** are used interchangeably.
- The term **user** refers to the end user in your organization who seeks access to cloud services and applications. Using the launchpad provided by Web Gateway, users submit credentials, open applications, and manage their accounts in the applications.
- The term **user interface** refers to the Web Gateway user interface where administrators configure the SSO service.
- The term **custom connector** refers to any cloud connector configured from a template. Web Gateway provides a range of connector templates. Some templates come with most, but not all, configuration built in. Other templates allow you to build cloud connectors from scratch.

Contents
- How cloud single sign-on is configured
- Considerations when exporting and importing the SSO rule set
- SSO process in proxy and non-proxy modes
- Supported authentication methods
- SSO Catalog of supported cloud services
- SSO Connector lists
- Providing SSO services for HTTP cloud applications
- Providing SSO services for SAML 2.0 cloud applications
- SAML authentication using an external Identity Provider
- Providing SSO services for .NET and Java web applications
- How the end user works with the application launchpad
- Customizing the application launchpad
- Creating bookmarks to cloud services for your organization
- Monitoring logons to cloud services on the dashboard
- Single Sign On rule set summary
- Single Sign On rule set reference
- SSO logging overview
- Resolving SSO issues
How cloud single sign-on is configured

To configure SSO access to cloud services and applications, complete the following high-level tasks.

SSO tasks require the Single Sign On rule set, which you import from the Rule Set Library. All SSO tasks can be performed using the default rules, settings, and lists visible in the key elements view of this rule set. To view the rules making up the rule set and create rules, settings, and lists of your own, unlock the key elements view.

Configuring single sign-on to some cloud services and applications requires configuration on the Service Provider side. Create an account in the Service Provider interface and complete the configuration steps there.

**Task**

1. Configure a method for authenticating users.

2. Import the Single Sign On rule set from the rule sets library and configure the rules.

   The Single Sign On rule set is located in the Cloud Services rule set group. You can configure the rules in the key elements view or click Unlock View to view configuration details as well as configure rules of your own.

3. Configure the Single Sign On settings for the Single Sign On module, which retrieves values and parameters for SSO properties and events in the Single Sign On rule set. This module comes with default settings named Default. In the SSO rules, properties and events that require these settings reference them using the notation <Default>. You can modify the default settings or create new settings.

   To locate these settings, select Policy | Settings | Engines | Single Sign On | Default.

4. For single sign-on to SAML and IceToken cloud services, configure an X.509 certificate and private key pair.

   To locate these settings, select Policy | Settings | Engines, then select SSO Certificates or SSO Private Keys, respectively.

5. Using SSO lists, you can configure custom cloud connectors from templates and lists of connectors to cloud services that users are allowed to access.

   - **SSO Host to Service ID mapping** — (Optional) Lets you map a name that is easy to remember (host name) to the Service ID of a configured custom connector.

     To locate this list, select Policy | Lists | Custom Lists | MapType.

   - **SSO Connector** — Lets you configure lists of connectors to services that users are allowed to access. You can add connectors to the default lists that come with the SSO service or create and configure lists of your own.

     To locate the SSO Services lists, select Policy | Lists | Custom Lists | SSO Connector.

   - **SSO Catalog** — Lets you view the predefined connectors and the custom connectors configured from templates. You can configure new connectors from templates, then view them in the Custom connectors list.

     To locate the catalog, select Policy | Lists | System Lists.

6. We recommend that you secure all launchpad communication with the HTTPS protocol. To do so, configure the Launchpad certificate settings used by the SSL Client Context without CA module, which handles certificates for SSL-secured communication.

   To locate the Launchpad certificate settings: In the key elements view, locate SSL Scanner settings, then click Edit.
To secure communication between Web Gateway and all cloud services with the HTTPS protocol, configure the SSL Scanner module settings. This step is required for proxy mode.

To require OTP authentication for SSO access to cloud services, enable OTP authentication, configure the OTP server settings, select an OTP delivery method, and configure the list of connectors to services that require OTP authentication.

`To locate these settings: In the key elements view, see the OTP Usage (One Time Passwords) section.`

To log SSO requests to the SSO access log instead of the general access log, enable SSO logging. To enable detailed logging for debugging purposes, enable SSO trace logging.

`To access these settings, select Policy | Rule Sets | Log Handler, then import the SSO Log rule set from the Logging rule set group in the Rule Set Library.`

Save the changes.

---

**Considerations when exporting and importing the SSO rule set**

The SSO rule set export and import does not include the SSO credentials required for accessing HTTP cloud applications or the Service IDs of custom connectors.

### SSO credentials (HTTP applications)

The SSO rule set is stored in the policy database. Importing the rule set updates the SSO policy. When you export or import the SSO rule set, the following information is included:

- All configured cloud connectors
- All configured connector lists
- All configured X.509 certificates and private key pairs

SSO credentials, which are required for accessing HTTP cloud applications and services, are stored in a separate database and are not part of the SSO policy. These credentials are not included in the export or import and must be re-created after the SSO rule set is imported.

When you back up the appliance configuration, you can include the SSO credentials in the backup. In this case, restoring the backup also restores the credentials.

### Service IDs (Custom connectors)

The Single Sign On module assigns numeric Service IDs to custom connectors at the time they are created from templates. These Service IDs are not included in the export of the SSO rule set. When the rule set is imported later, new Service IDs are assigned to the custom connectors.

After importing the SSO rule set, you must update any Service IDs that are used to reference custom connectors, as follows:
In the SSO Host to Service ID Mapping list, update the Key values to match the new Service IDs.

Some Service Providers, such as Gmail, include the Service ID in the SSO configuration. For these Service Providers, log on to your account and update the Service ID.

Failure to update the Service IDs after importing the SSO rule set can break custom connectors and links to cloud services and applications.

SSO process in proxy and non-proxy modes

The steps in the SSO process depend on whether the user’s credentials are submitted to the cloud application directly (non-proxy mode) or through Web Gateway (proxy or inline mode).

In proxy and non-proxy modes, Web Gateway authenticates the user, then presents the launchpad. The launchpad displays icons corresponding to the cloud applications the user is allowed to access. The SSO process appears the same to the user in both modes:

1. From a web browser on a client of Web Gateway, the user requests a launchpad.
2. After authenticating the user, Web Gateway sends a launchpad.
3. To open an application, the user clicks the icon corresponding to the application on the launchpad.
4. Web Gateway sends a logon form to the user.
5. If requesting access for the first time, the user is prompted for credentials, which the user provides and submits to Web Gateway. If requesting access for a second or later time, the logon form is automatically filled with the user’s credentials and submitted to Web Gateway.
6. If the credentials are valid, the user is allowed SSO access to the cloud application.

Proxy mode

In proxy mode, Web Gateway forwards the user’s credentials to the cloud application.

Figure 15-1  Single sign-on in proxy mode

When single sign-on takes place in proxy mode, Web Gateway can provide additional functionality that is not available in non-proxy mode:
• **Dynamic cloud applications** — Web Gateway can support HTTP cloud applications that provide logon page information dynamically, such as DropBox, by adding Javascript to the logon page. The Javascript completes the fields on the page with information.

• **Encrypted password** — The password is encrypted and hidden from the client computer.

**Non-proxy mode**

In non-proxy mode, the user's browser forwards the credentials to the cloud application.

![Figure 15-2  Single sign-on in non-proxy mode](image)

When single sign-on takes place in non-proxy mode, Web Gateway functions as a web server. When configuring your Domain Name Service and all SSO settings, you must use the IP address of the Web Gateway appliance in place of a host name.

**Supported authentication methods**

Generally, each cloud service or application uses one authentication method to log on end users.

Web Gateway provides SSO services for cloud applications that use HTTP or SAML 2.0 authentication. Web Gateway also provides SSO services for cloud applications using a proprietary authentication method implemented through a custom token named *IceToken*.

**Cloud connectors**

Web Gateway supports many HTTP and SAML 2.0 cloud applications with individual cloud connectors. A *cloud connector* is the configuration that allows Web Gateway to connect to and provide identity and SSO services for an application in the cloud. *Predefined cloud connectors* come fully configured with Web Gateway. *Cloud connector templates* come partly configured and require some configuration before they can be used.

**SSO data sources**

The data source from which Web Gateway obtains the end user’s credentials or information depends on whether single sign-on is to an HTTP or SAML service.

• **HTTP services** — Web Gateway uses an integrated credential store: a secure database that stores credentials like the user names and passwords required by HTTP services. Users who seek access to an HTTP service must first authenticate against the database.

• **SAML services** — Web Gateway retrieves identity information from an external data source and produces a SAML assertion attesting to the user’s identity.
SSO Catalog of supported cloud services

The SSO Catalog consists of all cloud applications and services supported by Web Gateway with cloud connectors. Connectors can be fully configured (predefined connectors) or templates that you can select and fully configure (custom connectors). The catalog also includes all connectors configured from templates by administrators. Connectors allow end users in your organization to access hundreds of cloud applications and services after authenticating one time.

A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for a cloud service or application. Each configured connector is saved in a file and includes information like the following:

- Information about the cloud service, such as name and category
- URLs needed for the SSO process
- Pages containing logon forms
- Data for generating the launchpad

Viewing the SSO Catalog

You can view the SSO Catalog in the user interface or in a technical note that can be downloaded in PDF format.

User interface

The user interface provides the most comprehensive and up-to-date view of the SSO Catalog. It includes all components making up the catalog: predefined connectors, connector templates, and custom connectors configured from connector templates by administrators.

The catalog is implemented as a system list. Like other system lists, it is updated between Web Gateway releases. Changes are delivered by update servers and can be viewed in the user interface. New connectors are added, and whenever possible, broken connectors are fixed. Connectors that are no longer supported are highlighted and the change is noted.

The system list consists of the following sublists. To view the sublists in the user interface, select Policy | Lists. In the Lists tree, expand System Lists | SSO Catalog.

- **Predefined connectors** — These connectors come fully configured with Web Gateway and only need selecting from the catalog.

- **Custom connectors** — These connectors are configured from templates that come with some, but not all, configuration built in. Custom connectors require configuration before they can be added to the catalog and selected.

In the user interface, predefined connectors and connector templates are organized by the names of the cloud applications and services they support. Custom connectors configured from connector templates are organized by the names that you specify.

To view the connector templates from which you configure custom connectors, select Policy | Lists. In the Lists tree, expand System Lists | SSO Catalog. Select Custom connectors, then click the Add icon. In the Add Connector dialog box, open the Template drop-down list. Notice that the generic connector templates are at the top of the list.

Custom connectors include any connector that you configure from a template for your situation. Connectors configured from generic templates (like generic HTTP and generic SAML 2.0) are custom connectors.

Technical note

The technical note is a snapshot of the SSO Catalog taken each time there is a major release of Web Gateway. It is not updated each time there is a release of the SSO Catalog.
The technical note lists all predefined connectors and connector templates in a single location. It includes the authentication method used by each service and optionally, a note describing the status of the service. For example, if a connector is no longer supported or has been renamed, this status is noted.

The technical note does not include custom connectors, which do not exist until they are configured from a connector template by an administrator.

**SSO Catalog in the user interface**

Predefined and custom connectors are listed in table format. While the tables include the same information, the details differ for each type of list.

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Displays the logo that represents the cloud application or service. When configuring a custom connector, you can specify a custom image.</td>
</tr>
</tbody>
</table>
| Name           | Uniquely identifies the predefined connector or custom connector instance.  
  • **Predefined connectors** — Displays the name of the cloud application or service and can include spaces.  
    Example: Air Canada  
  • **Custom connectors** — Displays the name that you configure for each connector instance.  
    From one connector template, you can configure multiple connector instances. For example, you can configure one connector instance for each user group and assign the instances different names, as follows:  
    • Google Calendar - IT  
    • Google Calendar - Sales |
| Description     | (Custom connectors) Allows you to provide a description for each connector instance. |
| Categories      | Specifies the type of service provided by the cloud application or service. When configuring a custom connector, you can change the default category or create a new one.  
  Examples: Collaboration, Marketing, Social |
| Service ID      |  
  • **Predefined connectors** — Specifies a name that uniquely identifies the predefined connector in the SSO Catalog. Typically, the service ID is the same as the name with the spaces removed.  
    Example: AirCanada  
  • **Custom connectors** — Specifies a number that uniquely identifies the custom connector in the SSO Catalog. This number is set by the Single Sign On module and cannot be changed. |
| Types           | Specifies the method that each cloud application or service uses to authenticate end users. Sometimes, applications and services are referred to by type, such as an HTTP application or a SAML service. This value is set by the Single Sign On module. |

**SSO Catalog as a service**

The SSO Catalog is a cloud service. As a cloud service, it is updated between Web Gateway releases.

The SSO Catalog is also known as the Connector Catalog as a Service (CCaaS).
Occasionally, a Service Provider changes the configuration details required for connecting to a cloud service or stops providing a cloud service altogether. These changes, which can break the connector to a service temporarily or permanently, require modifications to the SSO Catalog. Modifications, including new and fixed connectors, are delivered by update servers.

When the catalog is updated, an update message is displayed in the Web Gateway user interface. Broken connectors for which no resolution is planned are no longer supported and are flagged in the user interface as follows:

- **SSO Catalog**
  - **Connectors** — Predefined and custom connectors that are no longer supported are available for selection in the catalog. However, they are flagged with a yellow triangle and *No longer supported* message.
  - **Templates** — Templates for custom connectors that are no longer supported are available for selection in the catalog and can be configured. However, they are flagged with a yellow triangle and *No longer supported* message.

- **SSO Connector lists** — SSO Connector lists are custom lists of connectors to cloud services that end users are allowed to access. Connector lists containing connectors that are no longer supported are highlighted in yellow. Connectors in connector lists that are no longer supported are highlighted in yellow and flagged with *No longer supported* message.

### Generic vs. individual connector templates

Generic cloud connector templates support any cloud application that uses the specified authentication method. Because generic templates are more flexible than individual connector templates, they require more configuration.

#### Individual connector templates

Individual cloud connector templates provide the basis for configuring a connection to a specific cloud application. For example, the Salesforce connector template allows you to configure a custom connection to the Salesforce application in the cloud.

Because templates are configurable, you can create multiple custom connectors to a single cloud application such as Salesforce. To identify custom connectors, you assign them unique names.

#### Generic connector templates

Generic cloud connector templates allow you to configure a connection to any cloud application that uses the specified authentication method. For example, using the Generic HTTP Connector template, you can configure a connection to any cloud application that uses HTTP authentication to log on users. Generic templates allow you to configure connectors to cloud applications not found in the SSO Catalog.

Web Gateway provides generic cloud connector templates for the following authentication methods.

- **Generic HTTP connector** — Select this template when you want to configure a connector to an HTTP service that Web Gateway does not support with an individual connector.
- **Generic SAML2 connector** — Select this template when you want to configure a connector to a SAML 2.0 service that Web Gateway does not support with an individual connector.
- **Generic IceToken connector** — Select this template when you want to configure a connector to a service that uses an authentication method which Web Gateway does not support.
Configure a custom cloud connector using a template

After you configure a connector to a cloud service from a template, end users in your organization can access the service without authenticating more than one time.

**Task**

1. Select **Policy | Lists**.

2. In the **Lists** tree, expand **System Lists | SSO Catalog**, then click **Custom connectors**.

3. Click the **Add** icon.

   The **Add Connector** dialog box opens.

4. Provide values for the following fields and settings:
   - **Name** — Specifies a name that uniquely identifies the cloud connector instance.
   - **Description** — (Optional) Describes the cloud connector instance.
   - **Template** — From the drop-down list, select the template corresponding to the cloud service for which you want to configure SSO access.
     Template-specific settings open.
   - **Categories** — Specifies the type of service provided by the cloud service or application. When you select the template, a default value is loaded automatically. You can modify this value by clicking **Choose**.
   - **Browse** — Allows you to add or modify the logo that represents the cloud connector you are creating.

5. Configure the template-specific settings.

6. Click **OK**.

   The newly configured cloud connector is added to the SSO Catalog. To view the connector in the catalog, select **Custom connectors**.

Delete a custom cloud connector

You can remove a custom cloud connector from the SSO Catalog if it is not included in any SSO Connector list. Custom cloud connectors are connectors configured from templates.

Removing a custom cloud connector from the SSO Catalog removes all end user credentials entered for that connector. Recreating the connector with the same settings does not restore the user credentials that were lost when the connector was removed.

**Task**

1. Select **Policy | Lists**.

2. In the **Lists** tree, expand **System Lists | SSO Catalog**, then click **Custom connectors**.

3. Select the custom cloud connector you want to delete, then click the **Delete** icon.

   The **Confirm deletion** dialog box opens.

4. To confirm the deletion, click **Yes**.

   The custom cloud connector is removed from the SSO Catalog.
Locate information about the latest SSO updates

When working with the cloud single sign-on feature, you might want to know which version of the software and the catalog you are using. In the user interface, you can view the version number and date and time of the latest updates to the SSO feature or engine.

- **McAfee Single Sign On** — Updates include changes to the SSO software, for example, a change to an SSO rule.
- **McAfee SSO Connector Catalog** — Updates include changes to the list of cloud applications and services that Web Gateway supports with connectors.

<i> If you are not receiving SSO updates, confirm that you have a valid license. </i>

**Task**

1. Select **Dashboard | Charts and Tables | System Summary**.

2. To view the version numbers of the latest SSO updates: In the **Update Status** table, in the **Feature** column, locate the following rows:
   - McAfee Single Sign On
   - McAfee SSO Connector Catalog

3. To view the date and time of the latest SSO updates: In the **Last Update** table, in the **Engine** column, locate the following rows:
   - McAfee Single Sign On
   - McAfee SSO Connector Catalog

4. To refresh the view with the latest data, click the refresh icon in the upper right corner of the **Update Status** and **Last Update** tables.

**SSO Connector lists**

Web Gateway uses SSO Connector lists to control access to cloud services and applications.

**Configuring cloud access through SSO Connector lists**

Access to cloud services and applications is configured through lists of cloud connectors, each connector corresponding to a supported service in the SSO Catalog.

Some SSO Connector lists enable access. Other lists might require OTP authentication before access is permitted. Users are associated with lists through Web Gateway policies.

You can view the connectors in the catalog and select them when adding connectors to a connector list. The SSO Catalog organizes cloud connectors in two groups:

- **Predefined connectors** — These connectors come fully configured with Web Gateway and only need selecting from the catalog.

- **Custom connectors** — These connectors are configured from templates that come with some, but not all, configuration built in. Custom connectors require configuration before they can be added to the catalog and selected.

<i> Generic connectors are a special type of custom connector. </i>

Configuring access to a cloud service involves the following overall steps:
1 (Custom connectors) Configure a cloud connector to the cloud service you want users to access. The connector is added to the SSO Catalog.

2 Select the predefined or custom cloud connector from the SSO Catalog and add it to an SSO Connector list.

Add a cloud connector to an SSO Connector list
To control access to a cloud service, locate the corresponding cloud connector in the SSO Catalog and add it to an SSO Connector list.

Task
1 Select Policy | Lists.

2 In the Lists tree, expand Custom Lists | SSO Connector, then click the list you want to modify.

3 Click the Edit symbol.

A dialog box opens showing folders, each folder holding connectors in the specified category.

Example: Travel & Transportation

4 To add connectors to the list, select them individually or by category, then click OK.

   If the connector you want does not exist, you can create it by clicking Create new.

5 Click Save Changes.

Providing SSO services for HTTP cloud applications
Web Gateway supports many cloud services and applications that use HTTP authentication to log on end users with predefined cloud connectors or individual cloud connector templates.

A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for an application in the cloud. Web Gateway also provides a generic HTTP connector template, which can be configured for any cloud application that uses HTTP, but is not included in the SSO Catalog.

Before configuring a connector to an HTTP application, look up the application in the SSO Catalog. Predefined HTTP connectors come fully configured and only need selecting from the catalog. If the connector you want does not exist in the Predefined connectors or Custom connectors lists, you can create it from a template.

Most templates are partially configured connectors to specific cloud applications. If no template exists for your HTTP application, select the Generic HTTP Connector template. The generic HTTP template lets you configure connectors to HTTP applications that Web Gateway does not support with predefined connectors or connector templates.

Web Gateway supports single sign-on to dynamic HTTP applications that provide logon page information dynamically, such as DropBox, by adding Javascript to the logon page. Before the logon page can be modified, the SSO process must be running in proxy mode. In proxy mode, Web Gateway hides the real password from the client computer by replacing it with a token.

   Single sign-on to HTTP applications that are not dynamic can be implemented in proxy or non-proxy mode.
The SSO credential model for HTTP cloud applications

The SSO credential model for HTTP cloud services and applications supports individual end users who have more than one account in a cloud service or application. It also supports shared accounts, where multiple end users can access one or more cloud services or applications using the same credentials.

The following credential information is passed to most SSO properties and events:

- **Realm** — Specifies the name of the domain in which the current user is authenticated. The authentication domain can be an identity store, such as LDAP or Active Directory, or an authentication service.

- **User ID** — Identifies the current user. By default, the User ID has the same value as the Authentication.UserName property. You can modify the default value by mapping a different authentication attribute to the User ID.

- **Service ID** — Identifies a cloud service or application.

- **Account ID** — Identifies an individual or shared account in the cloud service or application.

Individual users are organized under realms or authentication domains. Users in an authentication domain are associated with one or more lists of cloud services or applications that they are allowed to access. For each cloud service or application, each user can have one or more accounts. The accounts can be individual accounts or shared.

Configure an HTTP cloud connector

Configure a connector to an HTTP service or application using a template.

**Task**

1. Select **Policy | Lists**.

2. In the **Lists** tree, expand **System Lists | SSO Catalog**, then click **Custom connectors**.

3. Click the **Add** icon.

   The **Add Connector** dialog box opens.

4. Provide values for the fields and settings common to all cloud connectors.

5. From the **Template** drop-down list, select the template corresponding to the HTTP service.

6. In the **Application Domain Name** field, specify the domain name of your instance of the HTTP service or application.

   Example: If your service URL is https://myorg.cloudapp.com, **myorg** is the name of your application domain.

7. Click **OK**.

The newly configured HTTP connector is added to the **SSO Catalog | Custom connectors** list.

Configure a generic HTTP cloud connector

Configure a generic HTTP cloud connector when you want to connect to an HTTP service that Web Gateway does not support with an individual connector.

**Task**

1. Select **Policy | Lists**.

2. In the **Lists** tree, expand **System Lists | SSO Catalog**, then click **Custom connectors**.

3. Click the **Add** icon.

   The **Add Connector** dialog box opens.
4. Provide values for the fields and settings common to all connectors.
5. From the **Template** drop-down list, select **Generic HTTP Connector**.
6. To configure a connector to a dynamic HTTP cloud service, select **Dynamic service**.
7. From the drop-down list, select the HTTP method that specifies how the form is sent.
8. In the **https://** field, specify where to send the form in URL format.
9. For each attribute sent in the form, configure one form field.
10. For each form field whose source is the credential store, configure one launchpad field.
11. (Optional) Configure one or more logon pages.
   - Dynamic HTTP cloud services require one logon page. Some cloud services require more than one logon page.
12. (Optional) Configure the fields on the logon page.
   - You only need configure the logon fields when they are different from the form fields.
13. To configure another generic HTTP connector, click **New Sign On Request**.
14. To save the HTTP connector configuration, click **OK**.

The newly configured generic HTTP connector is added to the **SSO Catalog | Custom connectors** list.

---

### Providing SSO services for SAML 2.0 cloud applications

Web Gateway supports cloud services and applications that use SAML 2.0 authentication to log on end users by providing cloud connector templates.

A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for an application or service in the cloud. Web Gateway provides connector templates for many individual cloud services and applications. Web Gateway also provides a generic SAML2 connector template. The generic template can be configured for any cloud service or application that uses SAML 2.0, but is not included in the SSO Catalog.

- Configuring single sign-on for a SAML 2.0 cloud application requires configuration in your SAML 2.0 application administrator account as well as in the Web Gateway user interface.

### How SAML single sign-on is initiated

The SAML SSO process can be initiated by the Identity Provider (IdP) or the Service Provider (SP).

The **Identity Provider** is the service that authenticates the end user. The **Service Provider** is the SAML cloud service or application that the end user wants to access. In the following examples of SAML single sign-on, Web Gateway performs the Identity Provider role.

The SSO process begins when the user requests access to a SAML application in the cloud. Web Gateway authenticates the user, then redirects the authentication result to the SAML application through the user’s browser. The redirected messages are automatic and take place quickly, so that the user is not aware of the authentication process running in the background.

#### IdP-initiated SAML single sign-on

Web Gateway initiates the SSO process, which consists of the following overall steps:
1. Web Gateway authenticates the user.

2. Web Gateway presents the user with a launchpad that includes icons for all SAML applications the user is allowed to access. The user requests access to a SAML application (the Service Provider) through Web Gateway (the Identity Provider) by selecting an icon on the launchpad.

3. Web Gateway redirects the authentication result to the SAML application through the user's browser.

4. The SAML application grants access to the user.

---

**SP-initiated SAML single sign-on**

The SAML application in the cloud initiates the SSO process, which consists of the following overall steps:

1. The user requests access to a SAML application (the Service Provider) directly.

2. The SAML application redirects the user's request to Web Gateway (the Identity Provider) through the user's browser.

3. Web Gateway authenticates the user.

4. Web Gateway redirects the authentication result to the SAML application through the user's browser.

5. The SAML application grants access to the user.
Pure SP-initiated SAML single sign-on
Not all SAML applications support IdP-initiated and SP-initiated single sign-on. Some SAML applications support only one. SAML applications that support only SP-Initiated single sign-on present a special use case called pure SP-initiated single sign-on.

1. Web Gateway authenticates the user.
2. Web Gateway presents the user with a launchpad that includes icons for all SAML applications the user is allowed to access. The user requests access to a SAML application (the Service Provider) through Web Gateway (the Identity Provider) by selecting an icon on the launchpad.
3. Because the SAML application only supports SP-initiated single sign-on, Web Gateway redirects the user's request to the application through the user's browser. Because the user is not authenticated, the SAML application redirects the user to Web Gateway with an authentication request.
4. Web Gateway redirects the authentication result to the SAML application through the user's browser.
5. The SAML application grants access to the user.

Certificate management for SAML single sign-on
SAML single sign-on requires an X.509 certificate and private key.
Together, the X.509 certificate and private key are known as the X.509 certificate key pair. The X.509 certificate contains the public key that makes up the key pair and a signature. The certificate can be self-signed or signed by a certificate authority.
The private key is used for signing outgoing SAML assertions and requests, and the X.509 certificate is used for verifying incoming signatures. The SSO party signing SAML assertions or requests with the private key provides the X.509 certificate to the SSO party verifying the signatures.

SAML services and applications have different certificate requirements. The following scenarios are common.

**Table 15-1 Certificate management**

<table>
<thead>
<tr>
<th>SSO process</th>
<th>Certificate management steps</th>
<th>SSO steps</th>
</tr>
</thead>
</table>
| IdP-initiated and SP-initiated SSO | 1. In the Web Gateway interface, the administrator generates or imports a private key and certificate pair and exports the certificate for use by the Service Provider.  
  2. In the Service Provider interface, the administrator uploads the certificate corresponding to the private key. | 1. Web Gateway creates signed SAML assertions attesting to the end user's identity using the private key.  
  2. The Service Provider uses the certificate to verify the signatures. |
| SP-initiated SSO                | 1. In the Service Provider interface, the administrator downloads the certificate corresponding to the private key.  
  2. In the Web Gateway interface, the administrator imports the Service Provider certificate. | 1. The Service Provider creates signed SAML SSO requests using the private key.  
  2. Web Gateway uses the certificate to verify the signatures. |

**Configure a SAML2 cloud connector**

Configure a connector to a SAML 2.0 service or application using a template.

**Task**

1. Select Policy | Lists.
2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3. Click the Add icon.
   
   The Add Connector dialog box opens.
4. Provide values for the fields and settings common to all connectors.
5 From the Template drop-down list, select the template corresponding to the SAML 2.0 service.

6 Provide values for the SAML settings.

7 Click OK.

The newly configured SAML2 connector is added to the SSO Catalog | Custom connectors list.

**Configure a generic SAML2 cloud connector**

Configure a generic SAML2 cloud connector when you want to connect to a SAML 2.0 service that Web Gateway does not support with an individual connector template.

**Task**

1 Select Policy | Lists.

2 In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.

3 Click the Add icon.

The Add Connector dialog box opens.

4 Provide values for the fields and settings common to all connectors.

5 From the Template drop-down list, select Generic SAML2 Connector.

6 Provide values for the generic SAML2 settings.

7 Click OK.

The newly configured SAML2 connector is added to the SSO Catalog | Custom connectors list.

**Configuring external data sources for SAML single sign-on**

While credentials for single sign-on to HTTP services are stored in the credential store that comes integrated with Web Gateway, SAML credentials come from external data sources, such as one or more LDAP servers, a database, or a web service. Several external data sources are configured using the external lists feature.

Identity information is fetched from external data sources as user attribute name-value pairs. The names must match the attribute names configured when the cloud connector was created.

---

**SAML authentication using an external Identity Provider**

To support organizations that want users to authenticate using a trusted, external Identity Provider, Web Gateway performs the SAML Service Provider role.

SAML authentication refers to how identity information is shared between the Identity Provider and the Service Provider.

In this SAML scenario, the external Identity Provider is a database or authentication service that the organization trusts, but is outside the Web Gateway system. Web Gateway sends a SAML authentication request to the external Identity Provider. The Identity Provider authenticates the user using any authentication method and returns the identity information in a SAML assertion in the SAML authentication response. Web Gateway extracts the identity information from the SAML assertion and sets a cookie, which the user can use to authenticate to a cloud application.
Internally, Web Gateway implements SAML authentication using an external Identity Provider through the authentication server and the proxy, which provides the SAML functionality that the authentication server is missing.

The application in the cloud provides a service and is also known as a Service Provider. However, in this scenario, the Identity Provider and Service Provider roles are assigned to the players in the SAML authentication process itself, not to the service provided in the cloud.

**SAML authentication process using an external Identity Provider**

The authentication server consumes the SAML assertion in the response sent by the external Identity Provider and sets a cookie for the authenticated user.

The SAML authentication process begins when the user requests access to an application in the cloud through Web Gateway. The process consists of HTTP Redirect (GET) and POST messages that are sent through the user’s browser (dashed lines). It also consists of messages that are sent and received by the user (solid lines). The messages that are sent through the user’s browser to another SAML party take place automatically and quickly. The user is not aware of the authentication process running in the background.

Web Gateway sends the SAML authentication request to and receives the SAML authentication response from the Identity Provider using the HTTP POST method.

Figure 15-6  SAML authentication process using an external Identity Provider

1. The user requests access to an application in the cloud through Web Gateway.
2. If Web Gateway does not recognize the user, the proxy redirects the request to the authentication server through the user’s browser.
3. The authentication server sends a SAML authentication request to the Identity Provider through the user’s browser. The Identity Provider authenticates the user and sends a SAML authentication response back to the authentication server, also through the user’s browser.
4. If the authentication server URL is static, the proxy intercepts the authentication response, constructs a dynamic URL, and redirects the response to the authentication server.
5. The authentication server consumes the SAML assertion in the response, sets a cookie, and redirects the authenticated user with the cookie to the application in the cloud through the proxy.
6. The proxy redirects the user with the cookie to the application in the cloud through the user’s browser.
7. The application grants access to the user.
How Web Gateway supports static ACS URLs

Web Gateway supports Identity Providers that do not support dynamic URLs by saving the dynamic ACS URL in the RelayState parameter.

**RelayState parameter**

The URL of the authentication server, which provides the Assertion Consumer Service, is dynamic. Not all Identity Providers support dynamic URLs, which contain parameters. Web Gateway supports these Identity Providers by saving the value of the dynamic ACS URL at the time the authentication request is created in the RelayState parameter.

> The RelayState parameter is configured automatically. No configuration is required on your part.

The authentication server sends the RelayState parameter and the authentication request to the Identity Provider in a POST form. When the Identity Provider returns the RelayState parameter and the authentication response, also in a POST form, the value of the RelayState parameter is unchanged.

If the ACS URL in the response is static, the proxy intercepts the response and restores the dynamic ACS URL from the static ACS URL and the RelayState value. Using the restored ACS URL, the proxy can redirect the SAML authentication response to the authentication server.

**Configuring a static ACS URL**

If the external Identity Provider supports dynamic URLs, the authentication server automatically sends the dynamic value to the Identity Provider and validates the ACS URL that it receives in return. No configuration is required in the Web Gateway interface.

If the external Identity Provider does not support dynamic URLs, the static ACS URL must be configured in two locations in the Web Gateway interface. The configured values must match.

- Static ACS URL value sent to the Identity Provider in the SAML request — This value is configured in the Prepare fixed ACS URL rule.
- Static ACS URL value expected in the SAML response from the Identity Provider — This value is configured in the SAML Response settings.

> The ACS URL value that you are expecting from the Identity Provider must also be configured at the Identity Provider.

**High-level configuration tasks**

Configuring SAML authentication with Web Gateway in the Service Provider role involves the following high-level tasks.

1. Import the Cookie authentication with SAML back end and fixed ACS URL rule set from the Rule Sets Library.
   > This rule set is located in the Authentication rule set group.

2. Configure a static ACS URL.
   > This task is required when the external Identity Provider does not support dynamic URLs.

3. Configure the SAML authentication request.
   > Web Gateway does not sign the SAML authentication request nor provide an X.509 certificate.

4. Configure the SAML authentication response. This task includes importing the X.509 certificate that the Identity Provider uses to sign the SAML authentication response and assertion.
To ensure that the authentication server recognizes the authentication response sent by the external Identity Provider, add the Identity Provider's service URL to the SAML IDP Whitelist.

Configure the SAML attributes that you want mapped to the Authentication.UserName and Authentication.UserGroups properties.

Manually configure the external Identity Provider to produce a SAML authentication response that meets the requirements you configure in the Web Gateway interface.

**Configure a static ACS URL**

Configure a static ACS URL when the external Identity Provider does not support dynamic URLs.

*Before you begin*

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

**Task**


2. Expand Cookie Authentication with SAML backend and fixed ACS URL | Cookie Authentication at Authentication Server, then select Authentication Server Request.

3. Select the rule Prepare Fixed ACS URL, then click Edit.

   The Edit Rule dialog box opens.

4. Select the step Events, select the event, then click Edit.

   The Edit Set Property dialog box opens with the User-Defined.SAMLUrlRewrite property selected.

5. Select "- enter your URL here -", then click Edit.

6. In the Enter a String dialog box, type the static URL, then click OK.

7. To close the Edit Rule dialog box, click Finish.

The static ACS URL is updated in the Authentication Server Request rule set view.

**Configure a SAML authentication request**

Configure the SAML authentication request that the authentication server sends to the external Identity Provider.

*Before you begin*

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

**Task**

1. Select Policy | Settings.

2. Expand Engines | SAML Request, then select SAML Request.

   The Authn Request window opens for configuration.

3. Provide values for the Authn Request settings.

4. Click Save Changes.
Configure a SAML authentication response

Configure the SAML authentication response that the authentication server expects to receive from the external Identity Provider. To determine whether the SAML authentication response is valid, the authentication server compares the actual values in the response to the configured values.

**Before you begin**

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

**Task**

1. Select Policy | Settings.
2. Expand Engines | SAML Response, then select SAML Response.
   The Authn Response window opens for configuration.
3. Provide values for the Authn Response settings.
4. Click Save Changes.

Add external IdP URL to SAML IdP Whitelist

To ensure that the authentication server recognizes the authentication response sent by the external Identity Provider, add the Identity Provider URL to the SAML IdP Whitelist.

**Before you begin**

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

**Task**

1. Select Policy | Lists.
2. Expand Custom Lists | Wildcard Expression, then select SAML IdP Whitelist.
3. Click Add.
   The Add Wildcard Expression dialog box opens.
4. In the Wildcard Expression field, specify an expression that matches the URL of the external Identity Provider.
5. Click OK.
   The matching expression is added to the SAML IdP Whitelist.

Configure SAML attribute mapping

You configure the names of the SAML attributes that you want mapped to the Authentication.UserName and Authentication.UserGroups properties.

**Before you begin**

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.
Task


2. Expand Cookie Authentication with SAML backend and fixed ACS URL | Cookie Authentication at Authentication Server, then select Authentication Server Request.

3. Select the rule Set user name and groups, then click Edit.
   
The Edit Rule dialog box opens.

4. Select the step Events, select an event, then click Edit.
   
The Edit Set Property dialog box opens with the Authentication.UserName or Authentication.UserGroups property selected.

5. Navigate to the Parameters for Property "Map.GetStringValue" dialog box.

6. Select an option:
   
   • Authentication.UserName — Select 2. Key (String) Value: "userid". Replace userID with the name of the SAML attribute that you want mapped to the user name property.
   
   • Authentication.UserGroups — Select 2. Key (String) Value: "userGroup". Replace userGroup with the name of the SAML attribute you want mapped to the user groups property.

7. To save your changes, click OK.

8. To close the Edit Rule dialog box, click Finish.

The names of the SAML attributes that you want mapped are updated in the Authentication Server Request rule set view.

Validating the SAML authentication response

To validate the SAML authentication response sent by the external Identity Provider, the authentication server compares the values in the response to the values configured in the Web Gateway interface.

You must manually configure the external Identity Provider to produce a SAML authentication response that meets the requirements configured in the Web Gateway interface.

To be valid, the SAML authentication response must meet the following requirements:

• The response must be a valid XML string.

• The response must include at least one SAML assertion.

• The <saml2p:StatusCode> element in the response must have the value Success.

• If configured, the response signature and assertion signature must be valid.
  
  • Response must be signed — If this setting is selected in the SAML authentication response configuration, the authentication server checks that the response is signed and that the signature is valid.
  
  • Assertion must be signed — If this setting is selected in the SAML authentication response configuration, the authentication server checks that the assertion is signed and that the signature is valid.

• The value of the <saml2:Issuer> element in the response must match the EntityID setting in the SAML authentication response configuration.

• The <saml2:Conditions> element in the response must include the attributes notBefore and notAfter.
• The current local time must fall within the specified time range, as follows.
  • **Response must be already valid** — When selected, this setting specifies that the current local time must be greater than or equal to the `notBefore` value.

  • **Negative clock skew** — The current local time must be greater than or equal to the `notBefore` time minus the negative clock skew value specified in the SAML authentication response configuration.

  • **Positive clock skew** — The current local time must be less than or equal to the `notAfter` time plus the positive clock skew value specified in the SAML authentication response configuration.

• If configured, the `audience` element must be included in the response and set to a predefined value, as follows.
  • **Audience must be set in the response** — If selected in the SAML authentication response configuration, the response must include the element `<saml2:Audience>`.

  • **Audience must match the predefined value** — If selected in the SAML authentication response configuration, the value of the `<saml2:Audience>` element must match the value specified in the Audience URI or ACS URL field in the configuration.

• The value of the `Destination` attribute in the `<saml2p:Response>` element in the response must match the ACS URL setting specified in the SAML authentication response configuration.

### Cookie authentication with SAML back end and fixed ACS URL — rule set

To support SAML authentication using an external Identity Provider, Web Gateway performs the Service Provider role. The rules in this rule set support this SAML scenario.

| Library rule set – Cookie authentication with SAML back end and fixed ACS URL |
| Criteria – Always |
| Cycles – Requests (and IM) |

This rule set contains the following nested rule sets:

• **Cookie authentication with SAML back end and fixed ACS URL**
  • Intercept SAML assertion if IdP uses a fixed ACS URL
  • Cookie authentication at HTTP(S) proxy
    • Set cookie for authenticated clients
  • Cookie authentication at authentication server
  • Authentication server request

This rule set contains the following rule.

#### Set client context

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Enable SSL Client Context without CA <code>&lt;Default Without CA&gt;</code></td>
</tr>
</tbody>
</table>

This rule secures all HTTP communication with the SSL protocol using the default certificate that comes with Web Gateway or one that you import. To configure the SSL certificate, click `<Default Without CA>`. 

Cloud single sign-on

SAML authentication using an external Identity Provider
**Intercept SAML assertion if IdP uses a fixed ACS URL**

The proxy intercepts SAML authentication responses containing a static ACS URL. It processes the SAML response and redirects the SAML assertion to the authentication server, which provides the Assertion Consumer Service.

### Nested library rule set – Intercept SAML assertion if IdP uses a fixed ACS URL

Criteria – Command.Name equals "POST" AND URL.Path is in list SAMLAuthResponseList

Cycles – Requests (and IM)

> To configure the list of fixed ACS URLs, click SAMLAuthResponseList.

This rule set contains the following rules.

#### Handle incoming SAML response

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set Authentication.Token = Request.POSTForm.Get (&quot;SAMLResponse&quot;)&lt;br&gt;Set Authentication.SAML.RelayState = Request.POSTForm.Get (&quot;RelayState&quot;)</td>
</tr>
</tbody>
</table>

The proxy retrieves the SAML response and RelayState parameter from the POST form sent by the external Identity Provider. It stores the response in the Authentication.Token property and the RelayState in the property Authentication.SAML.RelayState. When the Identity Provider does not support dynamic URLs, the proxy uses the URL returned in the RelayState to restore the dynamic authentication server URL.

#### Redirect SAML assertion to authentication server

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Block &lt;SAMLRedirectToAuth&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>

After restoring the dynamic authentication server URL, the proxy redirects the SAML assertion (stored in the Authentication.Token property) to the authentication server and sets the HTTP status code to 200 (OK). To provide custom settings for logging purposes, click <SAMLRedirectToAuth>.

#### Cookie authentication at HTTP(S) proxy

In the context of SAML authentication using an external Identity Provider, the proxy redirects requests that do not contain a valid cookie to the authentication server. The authentication server consumes SAML assertions and stores the user’s identity in a cookie.

### Nested library rule set – Cookie authentication at HTTP(S) Proxy

Criteria – Authentication.IsServerRequest equals false AND (Connection.Protocol equals "HTTP" OR Connection.Protocol equals "HTTPS") AND Command.Name does not equal "CONNECT" AND Command.Name does not equal "CERTVERIFY"

Cycles – Requests (and IM)
This rule set contains the following nested rule sets:

- Set Cookie for Authenticated Clients
- Authenticate Clients with Authentication Server

**Set cookie for authenticated clients**

After the authentication server consumes the SAML assertion and stores the user's identity in a cookie, it redirects the user with the cookie through the proxy to the requested application.

<table>
<thead>
<tr>
<th>Nested library rule set – Set cookie for authenticated clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsLandingOnServer equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

**P3P header to permit third party cookies in Internet Explorer**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Header.Block.Add (&quot;P3P&quot;, &quot;CP=&quot;NOI CUR OUR STP STA&quot;&quot;&quot;)</td>
</tr>
</tbody>
</table>

The P3P string is required for the Platform for Privacy Preferences Project (P3P). The string must match the privacy settings in the end user's browser. If the P3P string is not updated as shown in the table and the browser is Internet Explorer, processing fails.

**Set cookie and redirect client to the requested URL**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect&lt;Redirect Back From Authentication Server&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

The authentication server redirects the authenticated user with a cookie through the proxy to the requested application. To provide custom settings for logging purposes, click <Redirect Back From Authentication Server>.

**Authenticate clients with authentication server**

The proxy allows requests from external Identity Providers whose URLs are on the SAML IdP Whitelist and checks for a valid cookie in the requests. If none exists, the proxy redirects the requests to the authentication server.

<table>
<thead>
<tr>
<th>Nested library rule set – Authenticate clients with authentication server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.
Allow IDP requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL Domain matches in list SAML IdP Whitelist</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Rule Set</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

The proxy checks that the URL of the external Identity Provider making a request matches one of the URLs in the SAML IdP Whitelist.

To add URLs to the whitelist, click **SAML IdP Whitelist**.

Redirect clients that do not have a valid cookie to the authentication server

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate &lt;Local Cookie Authentication Server&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Authenticate &lt;Default&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the request from the external Identity Provider does not include a valid cookie, the proxy redirects the request to the authentication server. To configure a different authentication method, click **<Local Cookie Authentication Server>**. To provide custom settings for logging purposes, click **<Default>**.

Cookie authentication at authentication server

This rule set is a container for the Authentication server request rule set.

Nested library rule set – Cookie authentication at authentication server

Criteria – Always
Cycles – Requests (and IM)

This rule set contains the following nested rule set: Authentication server request.

Authentication server request

The rules in this rule set apply to the authentication server when it manages SAML authentication using an external Identity Provider. The authentication server processes the SAML authentication response, but does not set the cookie in this rule set. Cookie authentication is handled instead by the rules in the Cookie authentication at HTTP(S) rule set.

Nested library rule set – Authentication server request

Criteria – Authentication.IsServerRequest equals true
Cycles – Requests (and IM)

This rule set contains the following rules.

Redirect clients that have a valid cookie

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate &lt;Authentication Server - Cookie Check&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect &lt;Redirect Back From Authentication Server&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>
The authentication server redirects users having a valid cookie to the proxy. To change the cookie checking settings used by the authentication server, click `<Authentication Server - Cookie Check>`. To provide custom settings for logging purposes, click `<Redirect Back From Authentication Server>`.

### Prepare fixed ACS URL

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.SAMLUrlRewrite = URL.Protocol + &quot;://&quot; + URL.Host + &quot;- enter your URL here -&quot;</td>
</tr>
</tbody>
</table>

You can configure a static ACS URL for external Identity Providers who do not support dynamic URLs in this rule. If set, this value must match the ACS URL value configured in the SAML Response settings.

### POST SAML authentication request

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name does not match POST</td>
</tr>
<tr>
<td>Action</td>
<td>Block &lt;SAML request&gt;</td>
</tr>
</tbody>
</table>
| Events       | Set Authentication.SAML.RelayState = URL  
Set Authentication.Token = Authentication.SAML.CreateAuthnRequest  
(User-Defined.SAMLUrlRewrite)<SAML Request>  
HTTP.SetStatus (200) |

The authentication server sends the RelayState parameter and SAML authentication request in a POST form to the external Identity Provider. The RelayState parameter saves the value of the authentication server URL at the time the request is created. The request is created using values configured in the Web Gateway interface. The authentication server then sets the HTTP status code to 200 (OK). To change the SAML authentication request configuration, click `<SAML Request>` in this event.

### Handle SAML authentication response

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name equals &quot;POST&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | Set Authentication.Token = Request.POSTForm.Get ("SAMLResponse")  
Set Authentication.IsAuthenticated = Authentication.SAML.ParseAuthnResponse ("POST",  
User-Defined.SAMLUrlRewrite,  
Authentication.Token) <SAML Response> |

This rule retrieves the SAML response in the POST form sent by the external Identity Provider and stores it in the Authentication.Token property. It parses the response and returns a TRUE value if the response is valid and a FALSE value if it is not. To change the SAML authentication response configuration, click `<SAML Response>`.
Block invalid SAML response

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name equals &quot;POST&quot; AND Authentication.IsAuthenticated equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Block &lt;Authorized Only&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

After the SAML response is parsed, this rule checks the value of the property Authentication.IsAuthenticated. If the property is false, the SAML response is invalid and processing of the response is blocked. To provide custom settings for logging purposes, click <Authorized Only>.

Set user name and groups

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | Set Authentication.UserName = Map.GetStringValue (Authentication.SAML.Attributes, "userId") 


This rule maps the SAML attributes "userId" and "userGroup" to the Authentication.UserName and Authentication.UserGroups properties, respectively. You can use the rule editor to change the names of the SAML attributes that are mapped to the authentication properties.

Block empty user name

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.UserName equals &quot;&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Block &lt;Authorized Only&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the user name property is empty, this rule blocks processing of the response. To provide custom settings for logging purposes, click <Authorized Only>.

P3P header to permit third party cookies in Internet Explorer

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Header.Block.Add (&quot;P3P&quot;, &quot;CP=&quot;NOI CUR OUR STA&quot;)</td>
</tr>
</tbody>
</table>

The P3P string is required for the Platform for Privacy Preferences Project (P3P). The string must match the privacy settings in the end user's browser. If the P3P string is not updated as shown in the table and the browser is Internet Explorer, processing fails.

Redirect authenticated client back to proxy

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect &lt;Redirect Back From Authentication Server&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

Cloud single sign-on
SAML authentication using an external Identity Provider
According to the final rule in the rule set, the authentication server redirects the authenticated user back to the proxy. To provide custom settings for logging purposes, click <Redirect Back From Authentication Server>.

Providing SSO services for .NET and Java web applications

Using the Single Sign On rule set and the generic IceToken cloud connector template, you can configure single sign-on to any .NET or Java web application. Use this option when Web Gateway does not support the web application with a predefined connector or connector template.

Web Gateway implements single sign-on using the IceToken authentication method in the same way that it implements single sign-on using SAML authentication. Single sign-on using the two authentication methods has the following differences:

• In both cases, the Identity Provider sends the user information to the Service Provider in an assertion. The format of the user information in the assertion differs depending on the authentication method used.

• Single sign-on using the IceToken authentication method is simpler and easier to configure than single sign-on using SAML authentication.

Configure a generic IceToken cloud connector

To configure single sign-on to a .NET or Java web application, use the generic IceToken cloud connector template.

Task
1 Select Policy | Lists.
2 In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3 Click the Add icon.
4 The Add Connector dialog box opens.
5 Provide values for the fields and settings common to all connectors.
6 From the Template drop-down list, select Generic IceToken Connector.
7 Provide values for the generic IceToken settings.
8 Click OK.

The newly configured IceToken connector is added to the SSO Catalog | Custom connectors list.

How the end user works with the application launchpad

Using the application launchpad, the end user can open applications and select and manage application accounts.

Overall workflow

From the user's point of view, the launchpad workflow appears as follows:
1 Using the launchpad URL provided by an administrator, the user opens the launchpad.

2 The launchpad opens displaying the logon form, where the user enters credentials.

3 If authentication is successful, the launchpad presents icons representing the applications the user is allowed to access. To request an application, the user clicks the corresponding icon.

Opening the launchpad

Using the launchpad URL provided by an administrator, the user opens the launchpad from a web browser on a client of Web Gateway.

JavaScript must be enabled in the web browser.

The launchpad URL must contain the name of the management host configured in the Single Sign On settings. For example, if the host name is sso.mwginternal.com, the launchpad URL has one of the following values:

- https://sso.mwginternal.com
- https://sso.mwginternal.com/launchpad

Selecting a cloud application

Icons representing cloud applications are displayed in the left pane. When the user clicks an icon, the account information for that application is displayed in the right pane. If no account information is displayed, a couple of explanations are possible:

- **HTTP applications** — The first time an HTTP application is accessed, the user must provide credentials by clicking Add Account. The user also has the option of editing or deleting added accounts.

- **SAML applications** — Account information is not displayed or required, because SAML user information is retrieved from external sources.

You can initiate single sign-on to SAML applications and HTTP applications already configured with an account by clicking the application link in the left or right pane.

If the user has more than one account in an application, the icon representing that application is displayed multiple times in the left pane. Each icon is labeled with the user name corresponding to one account. To open a particular application account, the user can double-click the icon corresponding to the application-account pair.

Launchpad options

The launchpad provides options for displaying and selecting cloud applications and for working with application accounts. The following table describes these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application logos</td>
<td>Allow the user to select cloud applications.</td>
</tr>
<tr>
<td>Find application</td>
<td>Allows the user to type a string that filters the cloud applications displayed by name.</td>
</tr>
<tr>
<td>Display mode</td>
<td>From the drop-down list, the user selects a display mode:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Icons</strong> — Displays the application icons in rows.</td>
</tr>
<tr>
<td></td>
<td>- <strong>List</strong> — Displays the application icons in list format and includes the categories to which the applications belong.</td>
</tr>
</tbody>
</table>
Table 15-2  Launchpad options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort applications</td>
<td>From the drop-down list, the user selects a method for sorting the cloud applications: • By name — Displays cloud applications sorted by name. • By category — Displays cloud applications sorted by category and name.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the icon and name of the cloud application selected by the user.</td>
</tr>
<tr>
<td>Account</td>
<td>Displays the email address of the cloud application account selected by the user.</td>
</tr>
<tr>
<td>Edit Account</td>
<td>Allows the user to edit the selected cloud application account.</td>
</tr>
<tr>
<td>Add Account</td>
<td>Allows the user to add a cloud application account.</td>
</tr>
<tr>
<td>Web Gateway user</td>
<td>Displays the name of the user selecting the cloud application.</td>
</tr>
<tr>
<td>Category</td>
<td>Displays the category of the cloud application selected by the user.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of the cloud application account selected by the user.</td>
</tr>
<tr>
<td>Delete Account</td>
<td>Allows the user to delete the selected cloud application account.</td>
</tr>
</tbody>
</table>

The following account information is only available for HTTP applications. SAML user information is fetched from external sources.

Customizing the application launchpad

In the Web Gateway interface, you can specify a name and description for your organization, customize the look of the text, and import images of your organization and product logos. You can also customize the header, footer, and sidebar that frame the launchpad.

Opening the template editor

To customize the launchpad, you edit a collection of files and templates named Single Sign On Schema. To open the collection in a template editor, navigate to the Single Sign On default settings and select Single Sign On Schema from the Collection drop-down list.

Alternatively, you can access the templates directly by selecting the Templates tab.

Files in the /dat folder vs. /files folder

When generating the launchpad, the Single Sign On module uses files located in the following folders on the server where the appliance is installed and the SSO process is running:

- **/dat** — Files in this folder are system files maintained by the appliance. They are overwritten each time there is an update from the update server.
- **/files** — Files in this folder and subfolders, including /img, can be customized, because they are not overwritten by the update server.

Edit the Launchpad.html file

In the Launchpad.html file, you can specify a name and description for your organization and the names of the style sheet and the image files containing logos. You can also customize the header, footer, and sidebar that frame the launchpad.

For example, you can add a message of the day or links to your IT organization to the sidebar.
Task

1. Select Policy | Settings.

2. Expand Engines | Single Sign On, then select Default.
   The Single Sign On settings open.

3. From the Collection drop-down list, select Single Sign On Schema, then click Edit.
   The Template Editor opens with the Single Sign On Schema folder selected.

4. Expand Single Sign On Schema | Launchpad | en, then select html.
   The HTML Editor opens.

5. In the editor:
   a. Replace Your Company Name with the name of your organization.
   b. Replace Your Company Description with a description of your organization.
   c. (Optional) Replace customLaunchpad.css with the name of your custom .css file.
   d. Replace sample_logo.png with the name of the image file containing the logo that represents your organization.
   e. Replace productCompLogo.png with the name of the image file containing the logo that represents your product.

6. To customize the header, add content to the <div id="header"></div> element.
   Do not remove the "header" element even if it is empty.

7. To customize the footer, add content to the <div id="footer"></div> element.
   Do not remove the "footer" element even if it is empty.

8. To customize the sidebar:
   a. Add the <div id="aside"></div> element to the launchpad.html file, as follows.

   ```html
   <div id="main">
   <div id="aside">
   $SSO.GetDatFile("launchpadMain.html")$
   </div>
   </div>
   ```

   b. Add content to the <div id="aside"></div> element.

   Example:

   ```html
   <div id="aside">
   <img src="/files/img/your_logo.png">
   <hr>$first line of $SSO.GetDatFile("version.txt")$</hr>
   MWG: $MWG.Version$<br>$MWG.BuildNumber$
   </div>
   ```

   This example displays the logo you provide, the version number of the latest update from the update server, and the version and build numbers of the appliance in the sidebar.
9 To close the Template Editor, click **OK**.

10 Click **Save Changes**.

**Edit the default launchpad style sheet**

In the default launchpad style sheet that comes with the appliance, you can customize the look of your organization's name and description. You can also customize the header, footer, and sidebar that frame the launchpad.

For example, you can specify the background image that frames the launchpad. The image file can be located in the /files/img or /dat folder.

Alternatively, you can import a custom style sheet.

**Task**

1 Select **Policy** \* **Settings**.

2 Expand **Engines** \* **Single Sign On**, then select **Default**.

   The **Single Sign On** settings open.

3 From the **Collection** drop-down list, select **Single Sign On Schema**, then click **Edit**.

   The **Template Editor** opens with the **Single Sign On Schema** folder selected.

4 In the **File System** area, expand **singleSignOn**, then select **customLaunchpad.css**.

   The **Editor** opens.

5 In the editor, specify the font color, font-size, and font-family properties of your organization's name and description as you want them to look on the launchpad.

   **Example:**

   ```css
/* Organization Name */
#mainDesc
{
  color:RGB(51,51,51);
  font-size: 12pt;
  font-family:verdana;
}

/* Organization Description */
#subDesc
{
  color:RGB(102,102,102);
  font-size: 9pt;
  font-family:verdana;
}
```
6 In the editor, specify the background image that frames the launchpad.
In the following example, the background image can be a logo that is repeated until it fills the frame around
the launchpad.

```html
body {
  width: 100%;
}

#main {
  // In one of the following lines, replace <image_file> with the filename
  // of the background image and remove the comment tag from that line:
  // background: url("/files/img/<image_file>") repeat;
  // background: url("/dat/<image_file>") repeat;
  padding: 0px;
}

#aside {
  display: inline-block;
  width: 100px;
  align-self: flex-start;
}
```

7 To close the Template Editor, click OK.

8 Click Save Changes.

**Import a custom launchpad style sheet**
In the user interface, you can import a launchpad style sheet. It can be one that you exported and edited or one
of your own.

> When using your own style sheet, remember to place the .css file in the /files directory and to update the name of the .css file in Launchpad.html.

**Task**
1 Select Policy | Settings.
2 Expand Engines | Single Sign On, then select Default.
   The Single Sign On settings open.
3 From the Collection drop-down list, select Single Sign On Schema, then click Edit.
   The Template Editor opens with the Single Sign On Schema folder selected.
4 In the File System area, select singleSignOn.
5 From the Add drop-down list, select Existing File or Directory, browse for your style sheet file, then click Open.
   Your style sheet file is added to the File System under singleSignOn.
6 To close the Template Editor, click OK.
7 Click Save Changes.

**Provide a custom logo for the launchpad**
To provide a logo that represents your organization or product on the application launchpad, import a custom image file.

> Remember to place the image file in the /files/img or /dat folder and to update the name (and optionally the location) of the image file in Launchpad.html.
Task

1. Select **Policy | Settings**.
2. Expand **Engines | Single Sign On**, then select **Default**.
   
   The **Single Sign On** settings open.
3. From the **Collection** drop-down list, select **Single Sign On Schema**, then click **Edit**.
   
   The **Template Editor** opens with the **Single Sign On Schema** folder selected.
4. In the **File System** area, expand **singleSignOn**, then select **img**.
5. From the **Add** drop-down list, select **Existing File or Directory**, browse for the file containing your logo, then click **Open**.
   
   The image file is added to the **File System** under **img**.
6. To close the **Template Editor**, click **OK**.
7. Click **Save Changes**.

---

**Creating bookmarks to cloud services for your organization**

You can create bookmarks to cloud services or applications for users across your organization.

To create a bookmark, format the link as follows:

https://sso.mwginternal.com/login?service=<S>

Where `<S>` specifies the Service ID in the SSO Catalog.

When users click the link to the service, the SSO module delivers the HTML template for the logon page. The JavaScript in the HTML template retrieves the user’s account information for the specified service. Depending on the number of accounts the user has, one of the following actions takes place:

- The user has no account in the service — The user is redirected to the launchpad, which presents the option of creating an account. After creating an account, the user can log on to the service following the SSO process.
- The user has one account in the service — The user can log on to the service following the SSO process.
- The user has more than one account in the service — The user is redirected to the launchpad, which presents the option of selecting an account. After selecting an account, the user can log on to the service following the SSO process.

---

**Monitoring logons to cloud services on the dashboard**

On the dashboard in the user interface, you can view statistics about the number of logons to all cloud applications and services.

Select **Dashboard | Charts and Tables | Single Sign On Statistics** to view the following information:

- **All Logins** — Shows the number of logons to all cloud applications and services over the specified time period.
- **Logins per service** — Shows the number of logons by cloud application or service over the specified time period.
- **Logins per service** — Lists the specified number of cloud applications and services from most to least often accessed, including how many times each service was accessed.

- **Number of forbidden logins** — Shows the number of logons to all cloud applications and services over the specified time period that were denied because of invalid tokens.

---

## Single Sign On rule set summary

You configure and manage single sign-on through the Single Sign On rule set as well as related lists and settings.

The Single Sign On rule set comes with a default configuration that you can use and modify. When you first import and select the rule set, the default configuration opens in the simpler, locked view. You can configure and manage single sign-on using the locked view alone.

To access the more advanced view of the rule set, you unlock the view. If you unlock the view and find that you prefer the simpler, locked view, you cannot undo this action. To go back to the simpler, locked view, you must delete the rule set and import it again.

In the unlocked view of the default configuration, the nested rule sets are arranged and processed in the following order. Unless noted, all rule sets are enabled by default.

1. **Select Services** — Rules in this rule set add services to an internal map that determines whether the current user has access to the requested cloud service. The services are added from default lists that you configure.

2. **SSO Management** — This rule set contains the nested rule sets that manage single sign-on.

3. **Perform SSO** — This rule set contains the rule that processes the logon form.

The SSO Management rule set contains the following nested rule sets. They are arranged and processed in the order shown.

1. **HTTPS Handling** — Rules in this rule set secure all launchpad communication using the HTTPS protocol.

2. **Launchpad** — Rules in this rule set generate the application launchpad and logon page using the Single Sign On module settings.

3. **OTP Authentication** — Rules in this rule set enforce OTP authentication as a secondary authentication method. This rule set is disabled by default.

4. **Get Login Action** — This rule set retrieves information about the connector to the service that the user is requesting. For HTTP services, rule set processing stops. For other services, the rule set checks whether the user has the right to access the requested service.

5. **Process Common Tasks** — This rule set processes common SSO tasks using the Single Sign On module settings. It also contains the rule that blocks access to SSO resources that do not exist.

The Get Login Action rule set contains the following nested rule sets. They are arranged and processed in the order shown.

1. **Get Attributes on Premise** — Rules in this rule set fetch user information from an external LDAP data source for SAML single sign-on. The rule set only applies when Web Gateway is installed and running on premise.

2. **Get Attributes in the Cloud** — This rule set constructs the data needed for SAML single sign-on from the authenticated user name. It only applies when Web Gateway is installed and running in the cloud.
3 Perform SAML SSO — This rule set generates a response that contains the user information needed for completing single sign-on to the requested SAML service.

4 Perform IceToken SSO — This rule set generates a response that contains the user information needed for completing single sign-on to the requested service using the custom IceToken Web Gateway provides.

Single Sign On rule set reference

Using the nested rule sets that come with the Single Sign On rule set, you can configure SSO access to cloud services and applications for end users in your organization.

<table>
<thead>
<tr>
<th>Library rule set – Single Sign On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

The Single Sign On rule set contains the following nested rule sets:

- Select Services
- SSO Management
  - HTTPS Handling
  - Launchpad
  - OTP Authentication
- Get Login Action
  - Get Attributes on Premise
  - Get Attributes in the Cloud
  - Perform SAML SSO
  - Perform IceToken SSO
- Process Common Tasks
- Perform SSO

The rule sets nested in the SSO Management rule set are executed when the SSO.IsManagementRequest property returns a true value. This property is set to true in response to internal and external SSO requests, as follows:

- **Internal SSO requests** — The SSO.Action property returns a string value corresponding to an internal SSO request action.
- **External SSO requests** — An external SSO request is sent to the Web Gateway SSO service URL.

The rule sets nested in the Get Login Action rule set fetch user information and perform single sign-on to SAML cloud services and applications.
Select Services rule set
The rules in this rule set retrieve the specified list of cloud services, which the authenticated user or users of a shared account are allowed to access. The list and other information that you configure using the rules in this rule set are then available to the module for other SSO operations.

<table>
<thead>
<tr>
<th>Nested library rule set – Select Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

Add default SSO services (individual accounts)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.IsAuthenticated equals true AND String.IsEmpty(Authentication.UserName) equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.AddServices (&quot;defaultIDP&quot;, Authentication.UserName, Default SSO Services, {</td>
</tr>
<tr>
<td></td>
<td>&quot;label&quot;:&quot;Individual&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;permit-usage&quot;:&quot;yes&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;permit-management&quot;:&quot;yes&quot;</td>
</tr>
<tr>
<td></td>
<td>})&lt;Default&gt;</td>
</tr>
</tbody>
</table>

If the user is authenticated, the Single Sign On module retrieves the specified list of cloud services, which the user is then allowed to access.

The Single Sign On module executes the event with the following properties and settings:

- "defaultIDP" — Specifies the domain in the credential store where user account information is stored.
- Authentication.UserName — Specifies the name of the authenticated user.
- Default SSO Services — Specifies a list of services that the authenticated user is allowed to access.

- The following options form one parameter in JSON format:
  - "label" — Specifies the type of account: individual or shared.
  - "permit-usage" — Allows you to permit, deny, or require OTP authentication for access to the services on the list by the authenticated user. To configure access, specify the following values respectively: "yes", "no", or "otp".
  - "permit-management" — Allows you to permit, deny, or require OTP authentication for access to account management functions by the authenticated user. To configure access, specify the following values respectively: "yes", "no", or "otp".
  - <Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.
Add OTP secured SSO services (individual accounts, use after OTP authentication)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.IsAuthenticated equals true AND String.IsEmpty(Authentication.UserName) equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.AddServices (&quot;defaultIDP&quot;, Authentication.UserName, OTP Secured SSO Services, { &quot;label&quot;:&quot;Individual&quot;, &quot;permit-usage&quot;:&quot;otp&quot;, &quot;permit-management&quot;:&quot;otp&quot; })&lt;Default&gt;</td>
</tr>
</tbody>
</table>

If the user is authenticated, the Single Sign On module retrieves the specified list of cloud services. The user is allowed to access or manage these OTP-secured services after authenticating again with a one-time password entered on the launchpad.

The module executes the event with the following properties and settings:

- **defaultIDP** — Specifies the domain in the credential store where user account information is stored.
- **Authentication.UserName** — Specifies the name of the authenticated user.
- **OTP Secured SSO Services** — Specifies a list of services that the authenticated user is allowed to access after authenticating again with a one-time password.
- The following options form one parameter in JSON format:
  - **"label"** — Specifies the type of account: individual or shared.
  - **"permit-usage"** — Allows you to require OTP authentication for access to the services on the list by the authenticated user. Value: "otp"
  - **"permit-management"** — Allows you to require OTP authentication for access to account management functions by the authenticated user. Value: "otp"
- **<Default>** — Specifies settings for connecting to the SSO service provided by Web Gateway.

Add shared SSO services (shared accounts)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.AddServices (&quot;defaultIDP&quot;, &quot;sharedAccounts&quot;, Shared SSO Services, { &quot;label&quot;:&quot;Shared&quot;, &quot;permit-usage&quot;:&quot;yes&quot;, &quot;permit-management&quot;:&quot;yes&quot; })&lt;Default&gt;</td>
</tr>
</tbody>
</table>

The Single Sign On module retrieves the specified list of cloud services, which authenticated users of the shared account are then allowed to access.
• "defaultIDP" — Specifies the domain in the credential store where user account information is stored.

• "sharedAccounts" — Specifies a shared account.

• Shared SSO Services — Specifies a list of services, which authenticated users of the shared account are allowed to access.

• The following options form one parameter in JSON format:
  • "label" — Specifies the type of account: individual or shared.
  • "permit-usage" — Allows you to permit, deny, or require OTP authentication for access to the services on the list by users of the shared account. To configure access, specify the following values respectively: "yes", "no", or "otp".
  • "permit-management" — Allows you to permit, deny, or require OTP authentication for access to account management functions by users of the shared account. To configure access, specify the following values respectively: "yes", "no", or "otp".

• <Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

Handle single sign on using memorable hosts

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Map.HasKey (SSO Host to Service ID mapping, URL.Host) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect</td>
</tr>
<tr>
<td>Events</td>
<td>Set Redirect.URL = &quot;http://&quot; + SSO.ManagementHost&lt;Default&gt; + &quot;/login?service=&quot; + Map.GetStringValue (SSO Host to Service ID mapping, URL.Host)</td>
</tr>
</tbody>
</table>

If the SSO Host to Service ID Mapping includes the host name configured for the requested cloud service, the request is redirected to the URL configured for that service.

The Single Sign On module constructs the redirect URL from the specified string values and the following properties and settings:

• SSO.ManagementHost — Specifies the host name of the SSO service provided by Web Gateway.

• <Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

• Map.GetStringValue (SSO Host to Service ID Mapping, URL.Host) — Looks up the host name of the requested service in the SSO Host to Service ID map and returns the Service ID of that service.

HTTPS Handling rule set

This rule set secures SSO communication between the end user and the launchpad with the HTTPS protocol.

<table>
<thead>
<tr>
<th>Nested library rule set – HTTPS Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.
Enable SSL

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name equals &quot;CONNECT&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
</tbody>
</table>
| Events       | Enable SSL Client Context without CA <Launchpad certificate>  
                Enable SSL Scanner <Enable Content Inspection> |

If an SSO connection is required, this rule stops the request cycle. The Single Sign On module provides an SSL certificate and enables content inspection.

The module executes the events with the following settings:

- <Launchpad certificate> — Specifies the SSL certificate and settings. This certificate can be the default or one that you import.
- <Enable Content Inspection> — Specifies the settings that enable content inspection by the SSL Scanner module.

Enforce SSL

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Connection.Protocol equals &quot;HTTP&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect&lt;Default&gt;</td>
</tr>
</tbody>
</table>
| Events       | Set URL.Protocol = "https"  
                Set Redirect.URL = URL |

If the connection protocol is HTTP, the Single Sign On module sets the SSO protocol to "https" and the SSO request is redirected to the requested URL.

The rule executes the redirect action with the following settings:

<Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

Launchpad rule set

This rule set assembles all information needed for generating the launchpad or a logon page.

<table>
<thead>
<tr>
<th>Nested library rule set – Launchpad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

Create launchpad

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Path equals &quot;/&quot; OR URL.Path equals &quot;/launchpad&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO Launchpad&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>
If the requested URL specifies the SSO service or the launchpad, this rule generates the launchpad using the following settings:

**<SSO Launchpad>** — Specifies the language and template settings used to generate the launchpad.

We recommend that you do not modify the launchpad settings.

The Single Sign On module sets the HTTP status code to 200 (OK).

### Create automatic login page

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Path equals &quot;/login&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO Login Page&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>

If the requested URL specifies the SSO logon page, this rule generates the logon page, including the JavaScript, using the following settings:

**<SSO Login Page>** — Specifies the language and template settings used to generate the logon page.

We recommend that you do not modify the logon page settings.

The Single Sign On module sets the HTTP status code to 200 (OK).

### Create automatic login page (compatibility with some services)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Path matches regex(/login-.+)</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO Login Page&gt;</td>
</tr>
</tbody>
</table>

This rule applies when the requested URL specifies the SSO logon page using the format "/login-<Service ID>" instead of the default format that the SSO service is expecting: "/login?service=<Service ID>". This rule generates the logon page using the following settings:

**<SSO Login Page>** — Specifies the language and template settings used to generate the logon page.

We recommend that you do not modify the logon page settings.

The Single Sign On module rebuilds the requested URL using the default format and sets the HTTP status code to 200 (OK).

Some SAML services do not allow query parameters in the IdP URL when single sign-on is SP-initiated.
OTP Authentication rule set

Enabling this rule set allows you to enforce OTP authentication as a secondary authentication method for end users who want to access cloud services and applications.

**Nested library rule set – OTP Authentication**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>SSO.OtpRequired&lt;Default&gt; equals true</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

The rules in this rule set are executed when the SSO action requires OTP authentication.

**Prepare OTP context**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.HasParameter (&quot;requestOTP&quot;) equals true OR URL.HasParameter (&quot;pledgeOTP&quot;) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Authentication.SendOTP&lt;OTP&gt;</td>
</tr>
</tbody>
</table>

If there is a request for a one-time password from an authenticated user, the Single Sign On module sends the password to the user. The types of OTP requests are:

- "requestOTP" — The user requests the one-time password through the McAfee OTP server.
- "pledgeOTP" — The user requests the one-time password through Pledge, an OTP client running locally on a computer or mobile device.

The module executes the event with the following settings:

<OTP> — Specifies settings for OTP authentication.

**Return OTP context**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.HasParameter (&quot;requestOTP&quot;) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (JSON.ToString (JSON.StoreByName (JSON.CreateObject, &quot;otp-context&quot;, JSON.FromString (Authentication.OTP.Context&lt;OTP&gt;))))) HTTP.SetStatus (403)</td>
</tr>
</tbody>
</table>

If there is a request for a one-time password from an authenticated user, this rule stops the request cycle. The Single Sign On module generates a response containing the OTP context in a JSON object. The OTP context is provided in a header field when the McAfee OTP Server responds with a one-time password.

The module executes this event with the following settings:

<OTP> — Specifies settings for OTP authentication.

The module sets the HTTP status code to 403 (Forbidden).
Verify delivered OTP

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate&lt;OTP&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
</tbody>
</table>
| Events       | HTTP.GenerateResponse  
                ("authentication-required":"delivered-otp")  
                HTTP.SetStatus (403) |

If OTP authentication fails, this rule stops the request cycle. The Single Sign On module generates a response specifying the authentication result and method. The method, delivered OTP, specifies delivery of the one-time password by the McAfee OTP Server.

The module executes this event with the following settings:

<OTP> — Specifies settings for OTP authentication.

The module sets the HTTP status code to 403 (Forbidden).

Enable this rule if one-time passwords are delivered by McAfee OTP Server.

Verify Pledge generated OTP

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate&lt;OTP&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
</tbody>
</table>
| Events       | HTTP.GenerateResponse  
                ("authentication-required":"generated-otp")  
                HTTP.SetStatus (403) |

If OTP authentication fails, this rule stops the request cycle. The Single Sign On module generates a response specifying the authentication result and method. The method, generated OTP, specifies generation of the one-time password by the Pledge OTP client.

The module executes this event with the following settings:

<OTP> — Specifies settings for OTP authentication.

The module sets the HTTP status code to 403 (Forbidden).

Enable this rule if one-time passwords are generated by the Pledge OTP client.

Get Login Action rule set

This rule set retrieves information about the connector to the requested cloud service or application. For HTTP cloud connectors, processing of the rule set then stops. For other cloud connectors, the rule set checks whether the user has the right to access the requested cloud service or application.

<table>
<thead>
<tr>
<th>Nested library rule set – Get Login Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – SSO.Action&lt;Default&gt; equals &quot;GetLoginAction&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.
Get connector info

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.sso-conn-info = SSO.GetConnectorInfo (String.ToSSOConnector (URL.GetParameter (&quot;service&quot;)))</td>
</tr>
</tbody>
</table>

The Single Sign On module retrieves information about the connector to the service the user is requesting and stores it as a JSON object in a local variable named sso-conn-info. This information includes the following:

- **Name** (string) — Specifies a user-defined name for the cloud connector.
- **Service ID** (string) — Uniquely identifies the cloud service or application.
- **Type** (string) — Specifies the authentication method used by the cloud service.
  Values: HTTP, SAML2
- **Inline** (Boolean) — If true, the cloud connector supports a dynamic HTTP cloud service, which requires single sign-on in proxy or inline mode.
- **Deprecated** (Boolean) — If true, the cloud connector is no longer supported.

Stop rule set for form based logins

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) equals &quot;http&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Rule Set</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the cloud connector type is HTTP, this rule stops the Get Login Action rule set.

Validate user’s access permissions

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>SSO.UserHasAccessToService (URL.GetParameter (&quot;realm&quot;), URL.GetParameter (&quot;user&quot;), URL.GetParameter (&quot;service&quot;), &quot;usage&quot;)&lt;Default&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO: User Has No Access To Service&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

This rule checks the "service" and "usage" parameters to verify that the user has the right to access the requested service or application. If the "service" parameter is empty or the "usage" parameter is set to "no", this rule blocks access to the requested service.

This rule is executed with the following settings:
- **<Default>** — Specifies settings for connecting to the SSO service provided by Web Gateway.
- **<SSO: User Has No Access To Service>** — Specifies the language and template settings used to generate the block message for the user.

### Get Attributes on Premise rule set

The rules in this rule set fetch user information from an external LDAP data source for SAML single sign-on. This rule set is disabled by default and only applies when Web Gateway is installed and running on premise and the SSO type is SAML2.

<table>
<thead>
<tr>
<th>Nested library rule set – Get Attributes on Premise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – InTheCloud equals false AND JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) does not equal &quot;HTTP&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

### Get additional attributes from LDAP

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | Set Authentication.RawUserName = Authentication.UserName  
Set User-Defined.sso-user-data = Authentication.GetUserGroupsJSON<LDAP Authentication> |

The Single Sign On module fetches information about the user from an external LDAP data source through the Authentication filter. It then stores the information as a JSON object in a local variable named `sso-user-data`. The user information consists of the attribute name-value pairs expected by the SAML service or application.

This event is executed with the following settings:

- **<LDAP Authentication>** — Specifies the Authentication module settings configured for the external LDAP data source.

### Get additional attributes from LDAP using External Lists

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.sso-user-data = ExtLists.JSON (Authentication.UserName, &quot;&quot;, &quot;)&lt;LDAP Source&gt;</td>
</tr>
</tbody>
</table>

The Single Sign On module fetches information about the user from an external LDAP data source through the External Lists module. It then stores the information as a JSON object in a local variable named `sso-user-data`. The user information consists of the attribute name-value pairs expected by the SAML service or application.

This event is executed with the following settings:

- **<LDAP Source>** — Specifies the External Lists module settings configured for the external LDAP data source.
Get Attributes in the Cloud rule set

This rule set constructs the data needed for SAML single sign-on from the authenticated user name. It is disabled by default and only applies when Web Gateway is installed and running in the cloud and the SSO type is SAML2.

### Nested library rule set – Get Attributes in the Cloud

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>InTheCloud equals true AND JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;).does not equal &quot;HTTP&quot;)</td>
<td></td>
</tr>
</tbody>
</table>

Cycles – Requests (and IM)

This rule set contains the following rule.

Populate user’s data from user name

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.IsAuthenticated equals true AND Authentication.UserName matches <em>@</em> AND JSON.Size (User-Defined.sso-user-data) equals 0</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.sso-user-data = JSON.StoreByName (User-Defined.sso-user-data, &quot;mail&quot;, JSON.FromString (Authentication.UserName))</td>
</tr>
</tbody>
</table>

This rule only applies when the user is authenticated, the user name is an email address, and the sso-user-data variable is empty. The rule stores the attribute name-value pair formed by "mail" and the user's email address as a JSON object in the sso-user-data variable.

Perform SAML SSO rule set

This rule set generates a response that contains the end user information needed for completing single sign-on to the requested SAML service or application.

### Nested library rule set – Perform SAML SSO

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td></td>
</tr>
</tbody>
</table>

Cycles – Requests (and IM), Responses, Embedded Objects

This rule set contains the following rule.

Get login action (SAML)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;).matches saml*</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (SSO.GetSAMLLoginAction (URL.GetParameter (&quot;service&quot;), User-Defined.sso-user-data)&lt;Default&gt;)</td>
</tr>
</tbody>
</table>

Cloud single sign-on
Single Sign On rule set reference
If the cloud connector type is SAML2, this rule stops the request cycle. The Single Sign On module generates a response containing the user information needed for completing single sign-on to the requested SAML service or application.

This event is executed with the following settings:

<Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

### Perform IceToken SSO rule set

This rule set generates a response that contains the end user information needed for completing single sign-on to the requested service or application.

**Nested library rule set — Perform IceToken SSO**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.

#### Get login action (IceToken)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) equals &quot;icetoken&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (SSO.GetIceTokenLoginAction (URL.GetParameter (&quot;service&quot;), User-Defined.sso-user-data)&lt;Default&gt;)</td>
</tr>
</tbody>
</table>

If the cloud connector type is IceToken, this rule stops the request cycle. The Single Sign On module generates a response containing the user information needed for completing single sign-on to the requested service or application.

This event is executed with the following settings:

<Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

### Process Common Tasks rule set

This rule set processes common SSO tasks and blocks access to SSO resources that do not exist.

**Nested library rule set - Block Management Requests**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

#### Process common tasks

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>SSO.ProcessTask&lt;Default&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

This rule processes common SSO tasks, such as credential management.
### Block invalid or unhandled management requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;File Not Found&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (404)</td>
</tr>
</tbody>
</table>

This rule blocks access to a requested resource, when the resource does not exist, and is executed with the following settings:

*<File Not Found>* — Specifies the language and template settings used to generate the block message for the end user.

The Single Sign On module sets the HTTP status code to 404 (Not Found).

### Perform SSO rule set

This rule set allows the end user to log on to an HTTP cloud service or application when single sign-on is implemented in proxy (inline) mode.

### Nested library rule set – Perform SSO

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.

### Process form login

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.ProcessFormLogin&lt;Default&gt;</td>
</tr>
</tbody>
</table>

The Single Sign On module processes the logon form that users complete to access HTTP cloud services or applications in proxy (inline) mode. The execution of the event depends on the step in the logon process, as follows:

- The user requests the logon form — The event adds JavaScript to the logon page, enabling single sign-on to dynamic HTTP cloud services, and replaces the real password with a password token.
- The user submits the logon form — The event replaces the password token with the real password.

The SSO module executes this event with the following settings:

*<Default>* - Specifies settings for connecting to the SSO service provided by Web Gateway.

### SSO logging overview

The SSO Log rule set generates the SSO access log, and optionally the SSO trace log, from information about SSO requests that the proxy stores in the SSO.LogAttributes property.

The SSO proxy stores information about internal and external SSO requests in the SSO.LogAttributes property. When SSO logging is enabled:
Internal requests are logged to the SSO access log instead of the general access log.

External requests, which come from outside Web Gateway, are logged to the general access log.

To enable SSO logging, import the SSO Log rule set from the Logging rule set group in the Rule Set Library. The SSO Log rule set consists of the following nested rule sets:

- **Access Log** — Logs error and info messages to the SSO access log file.
- **Trace Log** — Logs all messages to the SSO trace log file.
- **Stop Logging** — Stops the SSO Log rule set cycle.

The trace log is more detailed than the access log and is intended for debugging the SSO feature.

Enabling SSO logging involves these overall steps:

1. Add the SSO Log rule set to the Log Handler rule set tree.
2. Move the SSO Log rule set above the Default logging rule sets in the Log Handler tree. This step ensures that SSO requests are logged to the SSO access log before the general access log and that the logging cycle is then stopped.
3. (Optional) Enable SSO trace logging.

### Enable SSO logging

When you enable SSO logging, SSO requests are logged to the SSO access log instead of the general access log. You can also enable SSO trace logging.

If you enable trace logging, we recommend that you set the log level to Full. To locate the log level setting, select **Policy | Settings | Engines | Single Sign On | Default | Advanced Settings**.

#### Task

1. Select **Policy | Rule Sets | Log Handler | Default**.
2. From the Add drop-down list, select **Rule Set from Library**.
   - The Add from Rule Set Library dialog box opens.
3. Expand **Logging**, then select **SSO Log**.
4. If importing the rule set creates conflicts, click **Auto-Solve Conflicts**, click one of the following strategies, then click **OK**.
   - **Solve by referring to existing objects**
   - **Solve by copying and renaming to suggested**
   - The SSO Log rule set is added to the Log Handler tree.
5. In the Log Handler tree, move the SSO Log rule set above the Default rule sets.
6. (Optional) To enable detailed logging:
   - In the Log Handler tree, expand **SSO Log**, then select the Trace Log rule set.
   - In the configuration window, select the Enable checkbox.
SSO Log rule set reference

The SSO Log rule set is activated when the request is made by an SSO component, including the SSO.Client and SSO.Proxy components.

SSO Log rule set

<table>
<thead>
<tr>
<th>Library rule set – SSO Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – JSON.AsString (JSON.GetByName (SSO.LogAttributes, &quot;origin&quot;)) matches SSO.*</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

The SSO.LogAttributes property is a JSON object containing the SSO request attributes shown in the following table. The SSO Log rule set generates the SSO access log and optionally the SSO trace log from the attributes in the JSON object.

Table 15-3  SSO.LogAttributes property

<table>
<thead>
<tr>
<th>SSO request log attribute</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Specifies the name of the internal action performed in response to the SSO request. Examples include:</td>
</tr>
<tr>
<td></td>
<td>• LoadLaunchpad</td>
</tr>
<tr>
<td></td>
<td>• GetServices</td>
</tr>
<tr>
<td></td>
<td>• StartHTMLLogin, StartSAMLLogin, and StartIceTokenLogin</td>
</tr>
<tr>
<td></td>
<td>• AddCredentials, UpdateCredentials, and DeleteCredentials</td>
</tr>
<tr>
<td>config</td>
<td>Specifies the name of the settings used by the internal action performed in response to the SSO request.</td>
</tr>
<tr>
<td>message</td>
<td>Describes the SSO request.</td>
</tr>
<tr>
<td>origin</td>
<td>Specifies the source of the values that the proxy copies to the SSO.LogAttributes property. The source can be one of the following SSO components:</td>
</tr>
<tr>
<td></td>
<td>• SSO.Client — The proxy copies the values provided by the client (browser) to this property without checking them first.</td>
</tr>
<tr>
<td></td>
<td>• SSO.Proxy — The proxy checks the values provided by the client (browser) before copying them to this property.</td>
</tr>
<tr>
<td></td>
<td>SSO.Client values are used by developers when testing and debugging SSO features and are included in the SSO trace log. For security reasons, only values checked by the proxy (SSO.Proxy values) are included in the SSO access log.</td>
</tr>
<tr>
<td>level</td>
<td>Specifies the log level. Only SSO requests having a log level of four or less are included in the SSO access log. SSO requests having a log level higher than four are also included in the SSO trace log, which is more detailed. The log levels are:</td>
</tr>
<tr>
<td></td>
<td>• Off (0) — Logging is turned off.</td>
</tr>
<tr>
<td></td>
<td>• Error (1, 2) — Only error messages are logged.</td>
</tr>
<tr>
<td></td>
<td>• Info (3, 4) — Error and info messages are logged to the SSO access log file.</td>
</tr>
<tr>
<td></td>
<td>• Full (5, 6) — All messages are logged to the SSO trace log file.</td>
</tr>
</tbody>
</table>
Table 15-3  SSO.LogAttributes property (continued)

<table>
<thead>
<tr>
<th>SSO request log attribute</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Specifies the name of the cloud service in the SSO request.</td>
</tr>
<tr>
<td>outward</td>
<td>Specifies whether Web Gateway performs the web server role or the web server is external to Web Gateway. This attribute has one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• FALSE — Web Gateway is the destination of the SSO request and creates the SSO response. In this case, Web Gateway performs the role of a web server. For example, Web Gateway performs the web server role when the user accesses the launchpad.</td>
</tr>
<tr>
<td></td>
<td>• TRUE — The SSO request is directed to an external web server, which creates the SSO response. In this case, Web Gateway does not perform the role of a web server.</td>
</tr>
</tbody>
</table>

SSO Access Log rule set

If the Access Log rule set’s criteria are met, the rule in this rule set writes a log entry to the SSO access log file. Each SSO log entry corresponds to one SSO request. To meet the criteria, the SSO component making the request must be the proxy and the log level in the request must be less than or equal to four.

<table>
<thead>
<tr>
<th>Nested library rule set – Access Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – JSON.AsString (JSON.GetByName (SSO.LogAttributes, &quot;origin&quot;)) matches SSO.Proxy* AND JSON.AsNumber (JSON.GetByName (SSO.LogAttributes, &quot;level&quot;)) less than or equals 4</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.
Write sso_access.log

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | Set User-Defined.logLine = DateTime.ToWebReporterString + " " + Authentication.UserName + " " + String.ReplaceIfEquals (IP.ToString(Client.IP), "", ".") + " " + String.ReplaceIfEquals (Number.ToString(Response.StatusCode), "", ".") + " " + Request.Header.FirstLine + " " + "" + JSON.AsString (JSON.GetByName (SSO.LogAttributes, "action")) + " " + JSON.AsString (JSON.GetByName (SSO.LogAttributes, "service")) + " " + JSON.AsString (JSON.GetByName (SSO.LogAttributes, "message")) + " " + FileSystemLogging.WriteLogEntry (User-Defined.logLine)<SSO Access Log>

This rule creates the SSO access log entry, then writes the entry to the SSO access log file. The rule creates the log entry by retrieving the following information in string format and concatenating the strings:

- Date and time stamp in Web Reporter format
- User name
- Client IP address (if it exists)
- Status code in the response (if it exists)
- First line of the SSO request header
- Type of SSO request (action)
- Name of the cloud service in the SSO request (service)
- Description of the SSO request (message)

To open and configure the file system log settings, click <SSO Access Log>.

Cloud single sign-on
SSO logging overview
SSO Trace Log rule set

The rules in the Trace Log rule set build an SSO trace log entry and write it to the SSO trace log file. The trace log is more detailed than the access log and is intended for debugging the SSO feature.

The Trace Log rule set is disabled by default. When you enable trace logging, we recommend that you set the log level to Full. To locate the log level setting, select Policy | Settings | Engines | Single Sign On | Default | Advanced Settings.

### Nested library rule set – Trace Log

Criteria – Always
Cycles – Requests (and IM), Responses, Embedded Objects

This rule set contains the following rules.

#### Web reporter timestamp

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.logLine = DateTime.ToWebReporterString</td>
</tr>
</tbody>
</table>

This rule sets the SSO trace log entry equal to the date and time stamp in Web Reporter format.

#### Add all sso attributes

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.logLine = User-Defined.logLine + &quot; &quot; + JSON.ToString (SSO.LogAttributes) + &quot;&quot;</td>
</tr>
</tbody>
</table>

This rule adds the SSO log attributes in string format to the existing SSO trace log entry.

#### Add firstline for outward requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsBool (JSON.GetByName (SSO.LogAttributes, &quot;outward&quot;)) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>

If the SSO request is handled by an external web server, this rule adds the first line of the request header to the SSO trace log entry.
Add firstline

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>

This rule is disabled by default. When enabled, it adds the first line of the SSO request header to the SSO trace log entry for external and internal requests.

Write sso_trace.log

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>FileSystemLogging.WriteLogEntry (User-Defined.logLine)&lt;SSO Trace Log&gt;</td>
</tr>
</tbody>
</table>

This rule writes the SSO trace log entry to the SSO trace log file. To open and configure the file system log settings, click <SSO Trace Log>.

SSO Stop Logging rule set

The SSO Stop Logging rule set stops the logging cycle after internal SSO requests are logged to the SSO access log and before they can be logged to the general access log.

<table>
<thead>
<tr>
<th>Nested library rule set – Stop Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

This rule set contains one rule.

Avoid additional logging of internal SSO requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsBool (JSON.GetByName (SSO.LogAttributes, &quot;outward&quot;)) equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the SSO request is handled by Web Gateway internally, this rule stops the current cycle of the SSO Log rule set. This action prevents internal SSO requests from being logged to the general access log.

For this rule to be effective, you must add the SSO Log rule set to the Log Handler tree above the Default logging rule set.
## Resolving SSO issues

See the following table for SSO issues and ways to resolve them.

### Table 15-4  Resolving SSO issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The credential store fails to return credentials when requested.</td>
<td>Check the error log for credential store errors (34050–34090).</td>
</tr>
<tr>
<td>The end user cannot log on to the selected cloud service.</td>
<td>The connector to the service might be broken. Contact the SSO Catalog support team.</td>
</tr>
<tr>
<td>The end user cannot update credentials for a cloud service.</td>
<td>Check the order of the rules in the Single Sign On rule set. The Select Services rule set, which adds services to SSO Connector lists, must be located before the Manage Form Credentials rule set.</td>
</tr>
<tr>
<td>SAML single sign-on fails.</td>
<td>Possible reasons for SAML SSO failure are:</td>
</tr>
<tr>
<td></td>
<td>• Not all user information is provided — Some cloud applications require specific user attributes. To view the missing user attributes, check the error log for SSO errors (34000–34999).</td>
</tr>
<tr>
<td></td>
<td>• Single sign-on is not configured correctly — Verify that single sign-on is configured correctly in the Web Gateway user interface and in the SAML application administrator account.</td>
</tr>
<tr>
<td>When automatic downloading of SAML metadata is configured and the download fails, an error is returned stating that the requested service does not exist.</td>
<td>Possible reasons for this error are:</td>
</tr>
<tr>
<td></td>
<td>• The metadata is downloaded from an HTTPS URL without a trusted certificate.</td>
</tr>
<tr>
<td></td>
<td>• The signature in the SAML metadata file is incorrect.</td>
</tr>
<tr>
<td></td>
<td>• The SAML metadata file is missing the signature.</td>
</tr>
<tr>
<td>After importing the SSO rule set, one or more custom connectors or links to cloud services and applications are broken.</td>
<td>When the rule set is imported, new Service IDs are assigned to the custom connectors. Update any Service IDs that are used to reference custom connectors.</td>
</tr>
</tbody>
</table>

For more information about this error, see the file: `/opt/mcfc/log/mcfc.log`. 
Cloud storage encryption

When the users of your network work with data that is stored in the cloud using a cloud storage service, Web Gateway provides a function for encrypting this data, together with the corresponding function for decryption.

- **Cloud storage encryption** — When a user uploads data to a cloud storage service, the data can be encrypted.

- **Cloud storage decryption** — When a user downloads encrypted data from a cloud storage service, the data is decrypted to enable the user to work with it.

A suitable rule set is available from the rule set library on Web Gateway for configuring cloud storage encryption and decryption.

### Contents

- Encrypting and decrypting cloud storage data
- Configure encryption and decryption of cloud storage data
- Configure the settings for encrypting and decrypting data
- Decrypt cloud storage data manually
- Cloud Storage Encryption rule set

### Encrypting and decrypting cloud storage data

To enhance security when users of your network complete in-the-cloud activities, you can configure the encryption of data that a user uploads to a cloud storage service. When the data is downloaded, it is decrypted to allow the user to work with it.

A module of Web Gateway, known as the Cloud Storage Encryption module (also referred to as Cloud Storage Encryption filter or engine), handles both encryption and decryption of data, including the metadata. Encryption and decryption remain transparent to the user.

Encryption and decryption is performed for "top-level" data that is processed in the request and response cycles. Data that is embedded in a request or a response and, accordingly, processed in the embedded objects cycle, cannot be encrypted or decrypted.

To encrypt and decrypt data, the module uses a standard algorithm, which can be one of the following:

- AES-128
- AES-192
- AES-256

The algorithm is also known as *cipher*.

A password is also required as a parameter of the encryption or decryption process.

For performing this process, the module relies on service description files, which exist for each of the various cloud storage services.
The files provide information on how to handle different data formats, the methods that can be used in an upload or download request, for example, PUT or POST, and the URLs that are sent with requests to identify the locations where the data should be uploaded to or downloaded from.

Service description files are updated when a new version of Web Gateway is installed. It is not possible to download new versions of these files from an update server.

Encryption and decryption of data can be performed for the following cloud storage services:

- Box
- Dropbox
- Google Drive
- Microsoft SkyDrive

For the Box cloud storage service, encryption and decryption is supported when a web browser or a native Box client is used to upload and download data. For Dropbox, Google Drive, and Sky Drive, it is supported when upload or download is performed from a web browser.

**Configuring encryption and decryption**

To configure the encryption and decryption process, you need to implement suitable rules on Web Gateway. They are provided in the Cloud Storage Encryption rule set, which you can import from the library.

The rules in the library rule set control the Cloud Storage Encryption module and provide a default password for the encryption or decryption process. The rule set also contains an optional rule for logging the process.

The rule that controls the module for encryption applies if it is found that a request that was received on Web Gateway is a request for uploading data to one of the configured cloud storage services. Similarly, the rule that calls the module for decryption applies if a request for downloading data from one of these services has been received.

If one of the two rules applies, it triggers an event that lets the module perform the encryption or decryption process.

But whereas decryption is executed as soon as the rule processing module (rule engine) has actually found the relevant rule to apply, encryption is not executed before all the following rules have also been processed, including rules configured for processing in the embedded objects cycle.

This ensures the data that is sent with a request for uploading or downloading can be processed in unencrypted format by the other rules.

Module settings are implemented with the import of the library rule set, which you need to configure to specify the following:

- Algorithm (cipher) used for encryption and decryption
- Supported cloud storage services
Data trickling and decryption

If data trickling is implemented as a mode of transferring data, decryption of an encrypted file that is downloaded from a cloud storage service might fail. You should therefore configure these functions as follows:

• On the rule set tree, the Cloud Storage Encryption rule set should be placed immediately before or after the rule set that you use to implement data trickling.

  This prevents rules of other rule sets from being processed between the decryption and the data trickling rules, which can cause the decryption to fail.

  A rule for enabling data trickling is contained in the Progress Indication rule set, which is an embedded rule set of the Common Rules rule set of the default rule set system.

To be completely sure that data trickling does not lead to a failed decryption, you can additionally do the following:

• Replace the **Always** in the criteria of the data trickling rule by **CloudEncryption.IsDecryptionSupported equals false**.

  This prevents data trickling from being started when downloaded data is decrypted. However, configuring the criteria like this will have an impact on the performance of the data trickling process.

Multiple encryption of data

When a request for uploading data to a cloud storage service is received, the data can be encrypted more than once, performing encryption differently each time.

For each encryption, you need to configure a rule. You can, for example, specify a password for a user group in one rule and let encryption be performed under a particular algorithm, which you also specify in that rule, and then specify a password for an individual user in the next rule and let encryption be performed under a different algorithm.

So when it comes to downloading the data, it can only be decrypted if both passwords are known.

To decrypt what has been encrypted in multiple rules, the same number of rules for decryption is needed. Algorithms and passwords must be the same as in their encryption counterparts and the order of these rules must be the reverse of the order in which you placed the encryption rules.

SSL-secured upload and download requests

To cover also requests for uploading data to a cloud storage service or for downloading data when they are sent using an SSL-secured connection, you need to make sure the SSL Scanner rule set is enabled.

This rule set is implemented in disabled state with the default system of rule sets for Web Gateway.

The certificates that are needed for communication over SSL-secure connections must be installed on the web browsers that users work with to send upload and download requests.

Manual decryption of data

When Web Gateway is temporarily unavailable in your network or when a password conflict arises, it could be required that you decrypt cloud storage data manually.

This can be done if you know the algorithm and password that were used when the data was encrypted. You can download the data directly from the cloud storage service to your system and run a command for manual decryption on this system, which includes algorithm and password parameters.
Monitoring encryption and decryption on the dashboard

Statistics about activities performed for encrypting and decrypting cloud storage data can be monitored on the dashboard of the user interface.

The following parameters are shown:

- Number of encryption and decryption operations and errors (over time)
- Volume of encrypted and decrypted data (over time)
- Number of encryption and decryption operations and errors per cloud storage service
- Volume of encrypted and decrypted data per cloud storage service

Configure encryption and decryption of cloud storage data

To configure the encryption and decryption of data that is uploaded to a cloud storage service or downloaded, complete the following high-level steps.

**Task**

1. Import the *Cloud Storage Encryption* rule set from the rule set library.
   - The rule set is located in the *Cloud Services* rule set group.
2. Configure the settings for encrypting and decrypting cloud storage data.
3. Ensure communication for encrypting and decrypting data can go on in SSL-secured mode.
   a. Enable the *SSL Scanner* rule set in the default rule set system of Web Gateway.
   b. For the browsers on the clients of Web Gateway that upload and download cloud storage data, make sure the certificates needed for SSL-secured communication are installed.
4. Save your settings.

Configure the settings for encrypting and decrypting data

To configure the settings for encrypting and decrypting cloud storage data, work with two different module (engine) settings.

**Task**

1. Select *Policy | Settings*.

2. On the *Engines* branch of the settings tree, expand *Cloud Storage Encryption* and select the particular settings for the Cloud Storage Encryption module you want to configure, for example, the *Default* settings.
   - The settings appear in the settings pane.
3. Configure these settings as needed.
4. Expand *Cloud Storage Encryption Support* and select the particular settings for the Cloud Storage Encryption Support module you want to configure, for example, the *Default* settings.
   - The settings appear in the settings pane.
5 Configure these settings as needed.

6 Click Save Changes.

Decrypt cloud storage data manually

When you cannot use Web Gateway to decrypt cloud storage data, you can perform the decryption manually by running a suitable command if you know the algorithm and password that were used for the encryption.

**Task**

1 Download the data in encrypted format from the cloud storage service that stored the data to your system.

2 Run the following command to decrypt the data:

   openssl enc -<cipher> -d -in <encrypted file> -out <decrypted file> -k <password> -md sha256

   The variable parameters have the following meanings:

   - `<cipher>`: Algorithm used to encrypt the data
   - `<encrypted file>`: Path and file name for the file that contains the encrypted data
   - `<decrypted file>`: Path and file name for the file the decrypted data should be written to
   - `<password>`: Password used when the data was encrypted

   The data is decrypted and written to the specified file.

Cloud Storage Encryption rule set

The Cloud Storage Encryption rule set is a library rule set for encrypting and decrypting data that is uploaded to and downloaded from cloud storage services.

<table>
<thead>
<tr>
<th>Library rule set – Cloud Storage Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**Set encryption password**

*Always* → Continue – Set User-Defined.Encryption Password = “webgateway”

The rule uses an event to set the default password for Web Gateway as the password that is used when data is encrypted.

**Enable encryption**


The rule uses the CloudEncryption.IsEncryptionSupported property to check whether encryption of data can be performed. If this is the case, an event is used to perform the encryption.

**Enable decryption**


The rule uses the CloudEncryption.IsDecryptionSupported property to check whether decryption of data can be performed. If this is the case, an event is used to perform the decryption.
Fix content type after decryption

CloudEncryption.IsDecryptionSupported<Default> equals true –> Continue – MediaType.Header.FixContentType

The rule uses the CloudEncryption.IsDecryptionSupported property to check whether a decryption of cloud storage data was performed.

If this is the case, an event is used to modify the Content-Type field in the header of the response that was sent to deliver the data to Web Gateway. Cloud storage services set this field by default to application/octet-stream, as they are not able to recognize real media types when data is encrypted. The MediaType.Header.FixContentType event sets the field to a value for a real media type.

This rule fixes the issue that cloud storage services set this field by default to application/octet-stream, as they cannot recognize different media types when data is encrypted. The MediaType.Header.FixContentType event sets the field to a value for the real media type.

The rule is not enabled by default.

Log encryption password

CloudEncryption.IsEncryptionSupported<Default> equals true –> Continue –

Set User-Defined.encrypt-log. =
DateTime.ToGMTString
+ ", User: "
+ Authentication.UserName
+ ", IP: "
+ IP.ToString (Client.IP)
+ ", Service: "
+ CloudEncryption.ServiceName
+ ", Cipher: "
+ CloudEncryption.CipherName<Default>
+ ", Password: "
+ User-Defined.EncryptionPassword
FileSystemLogging.WriteLogEntry (User-Defined.encrypt-log)<Encryption Log>

The rule uses an event to create a log entry for an encryption.

A second event is used to write this entry into the log called Encryption Log, which is specified by the event settings. Since data is written into the log in encrypted format, you need a password to access it (default password: webgateway).

The rule is not enabled by default.
Hybrid solution

A Web Protection license provides all components needed to set up the hybrid solution. When the hybrid solution is configured and enabled, the Web Gateway policy is pushed to McAfee WGCS at the synchronization interval you specify.

Using the hybrid solution, you can:

• Apply one policy across your organization.

• Ensure that the policy is updated in the cloud when it is changed on premise through configured synchronization intervals or manual synchronization.

Contents

- On-premise and remote web access
- Components of the hybrid solution
- How the hybrid solution works
- Authentication considerations for the hybrid solution
- Why some rules are restricted
- Managing the hybrid solution

On-premise and remote web access

The hybrid solution provides web protection for your organization whether users are working inside or outside your local network.

• On-premise access — Users who access the web from systems that are physically installed on your local network are working on premise. This term extends to users who are connected to your network by a virtual private network (VPN) interface.

  Web Gateway protects your organization when users make web requests while working on premise.

• Remote access — Users who access the web from systems that are not connected to your local network, for example, while traveling or working in a public location, are working remotely.

  McAfee WGCS protects your organization when users make web requests while working remotely.

Components of the hybrid solution

The hybrid solution integrates McAfee components installed on your network with McAfee cloud services.

If you require a hardware platform to run Web Gateway, the hardware is a separate purchase.

Components of the hybrid solution include:
• Web Gateway — This hardware-based or virtual appliance is installed locally on your organization's network. The on-premise appliance protects your network from threats that might arise when users access the web from inside the network. The appliance has its own interface, where administrators manage the product.

• McAfee WGCS — This cloud service protects your network from threats that might arise when users access the web from inside or outside the network. The service is managed with McAfee ePO Cloud.

• Client Proxy — This software, when installed on the endpoint, is aware of the user's location and redirects network traffic or lets it pass, accordingly:
  • Inside the network or connected to the network by VPN — Client Proxy lets network traffic pass to Web Gateway for filtering.
  • Outside the network — Client Proxy redirects network traffic to McAfee WGCS for filtering.

Client Proxy can be managed with McAfee ePO, McAfee ePO Cloud, or both depending on the setup.

• Content Security Reporter — This extension, which is managed with McAfee ePO, allows you to view web traffic and usage trends consolidated from Web Gateway and McAfee WGCS logs.

• McAfee ePO — This management platform, which is installed on your network, allows you to manage Client Proxy and Content Security Reporter.

• McAfee ePO Cloud — This cloud-based management platform allows you to manage McAfee WGCS and Client Proxy.

How the hybrid components are managed

This table summarizes how the hybrid components are managed with McAfee ePO and McAfee ePO Cloud.

<table>
<thead>
<tr>
<th>Hybrid component</th>
<th>Managed with McAfee ePO</th>
<th>Managed with McAfee ePO Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Gateway</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>McAfee WGCS</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Client Proxy</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Content Security Reporter</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

How the hybrid solution works

The on-premise and cloud components of the hybrid solution work together to protect your organization from threats that might arise when users access the web from inside or outside the network.

After the solution is configured and enabled, the Web Gateway policy is pushed to the cloud at the specified synchronization interval. The Policy Browser interface, where the McAfee WGCS policy is configured in the McAfee ePO management console, is disabled. A Policy Unavailable message displays information about the hybrid synchronization, such as the date and time of the last sync.

The following diagram shows how the key hybrid components are set up and connected. The diagram assumes that Client Proxy is managed with McAfee ePO and that the Client Proxy software is already installed on the McAfee ePO server and the endpoint.
Client Proxy credentials are configured using McAfee ePO, then exported and shared with McAfee ePO through an .xml file. These steps ensure that the Client Proxy policy is synchronized on premise and in the cloud.

1. Using the McAfee ePO management console, the administrator configures the Client Proxy shared password and exports the Client Proxy credentials to an .xml file.

2. Using the McAfee ePO management console, the administrator imports the Client Proxy credentials from the .xml file, then creates a Client Proxy policy for use with the hybrid solution. The administrator assigns the policy to all managed endpoints in the organization.

3. Managed endpoints can be located inside your organization’s network, connected to your network by VPN, or located outside your network. A typical Client Proxy policy redirects web requests made by users inside your network (or connected by VPN) to a Web Gateway appliance installed on your network. For users working outside your network, a typical policy redirects web requests to McAfee WGCS.
4 In the Web Gateway interface, the administrator reviews the web protection policy and enables the rule sets to be pushed to the cloud.

5 In the Web Gateway interface, the administrator configures and enables the hybrid solution. When the deployment is enabled, the Web Gateway policy is pushed to the cloud at the specified synchronization interval. The Policy Browser interface in the McAfee ePO management console is disabled.

The hybrid solution doesn't change how the Client Proxy policy is applied. The Client Proxy software installed on the endpoint continues redirecting web requests as before.

## Authentication considerations for the hybrid solution

McAfee WGCS authenticates users when they are working outside the network. Authentication settings configured on premise and in the cloud must be compatible.

### Group name format

Web Gateway and McAfee WGCS use different formats for the names of user groups. We recommend updating the format of the group names used on premise to match the format used in the cloud. Otherwise, the policy rules configured on premise might apply differently to users when they are working outside the network.

<table>
<thead>
<tr>
<th>Product</th>
<th>Group name formats used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Gateway</td>
<td>DomainName\GroupName</td>
</tr>
<tr>
<td></td>
<td>GroupName</td>
</tr>
<tr>
<td>McAfee WGCS</td>
<td>DomainName\GroupName (recommended)</td>
</tr>
</tbody>
</table>

To make sure that the group names used on premise include the domain name, review the rules and rule sets that are enabled in the cloud. If you are using Client Proxy as the authentication method, configure the Authentication with McAfee Client Proxy rule and select Keep domain name in group name.

### User name and user group properties

McAfee WGCS authenticates users when they are working outside the network and assigns values to the user name and user group properties according to the authentication method used. These properties correspond to the Authentication.UserName and Authentication.UserGroups properties in the Web Gateway interface.

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>The user is authenticated when...</th>
<th>Policy decisions are based on...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Proxy</td>
<td>Client Proxy is installed on the endpoint, a policy is deployed to the endpoint, and the user sends a web request from a managed computer.</td>
<td>Group memberships returned by Client Proxy</td>
</tr>
<tr>
<td>IP range</td>
<td>One or more IP address ranges are configured and the user sends a web request from one of the configured ranges.</td>
<td>Configured IP address ranges in McAfee WGCS</td>
</tr>
<tr>
<td>SAML</td>
<td>SAML authentication is configured and the user sends a web request to the SAML service port: 8084.</td>
<td>Group ID attribute value in the SAML assertion</td>
</tr>
<tr>
<td>IPsec site-to-site</td>
<td>Web requests are received through the IPsec VPN tunnel configured between your network and McAfee WGCS.</td>
<td>Membership in your organization</td>
</tr>
</tbody>
</table>
Why some rules are restricted

Not all Web Gateway rules be are compatible with McAfee WGCS.

Rule properties and events

Some rule properties and events cannot be used with McAfee WGCS. For example, events that increase counters, send emails to an administrator, or write entries to log files are not compatible with the cloud service.

In general, policy elements cannot be used in a hybrid solution if they:

- Rely on particular network components or external services — For example, mail services require a mail server, such as an SMTP server, SNMP properties require a trap sink, and next-hop proxy properties require next-hop proxy servers.
- Relate to functions that McAfee WGCS does not support — Examples include quota management and PDStorage functions and functions that require the exchange of runtime data, such as, between multiple Web Gateway appliances in a Central Management configuration.

In the Web Gateway interface, warning messages flag rules that are restricted.

- Properties — Pay attention to warnings about properties when they are set to their default values. These properties are not compatible with the hybrid solution and sometimes result in unexpected behavior.

  **Best practice:** Verify that rules having a property which is flagged with a warning work as expected when synchronized with McAfee WGCS.

- Events — You can ignore warning messages about events, because they are not executed and have no effect on the hybrid solution.

Sample warnings

The following sample warnings show rules that are restricted, because they contain a property or event that cannot be used with McAfee WGCS.

- A property is incompatible with McAfee WGCS — A warning is displayed, which identifies the rule and the property. It also contains a sentence like the following:

  Property PDStorage.GetAllData must not be used in SaaS.

- An event is incompatible with McAfee WGCS — A warning is displayed, which identifies the rule and the event. It also contains a sentence like the following:

  Event SNMP.Trap.Send.User(Number, String) must not be used in SaaS.

Managing the hybrid solution

After setting up the hybrid components, you manage the solution in the Web Gateway interface.

Management tasks include:

- Identifying rule sets that aren't supported in the cloud
- Enabling rule sets for hybrid synchronization
- Configuring and enabling the hybrid solution
- Verifying that policy synchronization succeeded
- Adding hybrid information to a block page

**Identifying rule sets not supported in the cloud**

Not all Web Gateway rule sets are compatible with the cloud. Incompatible rule sets can't be enabled in the cloud and synchronized with McAfee WGCS.

To identify which rule sets aren't supported in the cloud:

- View the rule sets in the Web Gateway interface — Select **Policy** | **Rule Sets**, then select an individual rule set. If the **Enable in Cloud** checkbox in the configuration pane is grayed out, the rule set isn't supported in the cloud.
- See the list of properties in Appendix A of the *McAfee Web Gateway Product Guide* — Any rule sets that use properties identified as *not SaaS-compatible* are not supported in the cloud.

**Enable rule sets for hybrid synchronization**

You must enable the Web Gateway rule sets that you want synchronized with McAfee WGCS.

**Before you begin**

Review the rule sets and decide which ones to enable in the cloud. The default rule sets provide all rules needed for the hybrid solution.

When you enable a rule set for hybrid synchronization, the rule set view determines whether nested rule sets are also enabled in the cloud.

- **Key elements view** — Nested rule sets are enabled.
- **Complete rules view** — When the rule set is enabled from the context menu, nested rule sets are enabled too. When the rule set is enabled in the configuration pane, nested rule sets are not enabled and must be enabled individually.

**Task**

1. In the Web Gateway interface, select **Policy** | **Rule Sets**.
2. For each rule set that you want synchronized with McAfee WGCS, select it, then select **Enable in Cloud**.
3. Click **Save Changes**.

The selected rule sets are enabled for synchronization with the cloud.

**Configure and enable the hybrid solution**

Configure the connection with McAfee WGCS and the synchronization interval.

**Before you begin**

The hybrid components are set up.

The Web Gateway rule sets that you want synchronized with McAfee WGCS are enabled in the cloud.

You have your McAfee ePO credentials and your McAfee WGCS customer ID.

After hybrid synchronization is enabled in the Web Gateway interface, it can't be disabled and the Web Protection policy in the cloud, which is overwritten, can't be restored. But you can manually control when the on-premise policy is synchronized with the cloud.
Task
1 In the Web Gateway interface, select Configuration | Appliances.
2 On the Cluster branch of the appliances tree, click Web Hybrid.
   The hybrid settings open in the configuration pane.
3 Configure the settings as needed.
4 Click Save Changes.

Hybrid synchronization is enabled, and the Web Gateway policy is pushed to McAfee WGCS at the specified synchronization interval or manually.

Verify that policy synchronization succeeded
To verify that the hybrid solution is correctly configured and that policy synchronization succeeded, you can perform the synchronization manually.

Task
1 In the Web Gateway interface, select Troubleshooting, then under the name of the appliance, select Synchronization to Cloud.
2 In the expanded list, select Synchronization to Cloud.
3 In the Synchronization to Cloud pane, click Synchronize.
   This message is displayed: Policy synchronization successfully performed!

Add hybrid information to a block page
You can add information to a block page that shows whether the on-premise appliance or cloud service blocked the user's request.
In a hybrid deployment, McAfee WGCS shares the block pages that are configured in the Web Gateway interface. Using the property InTheCloud, you can add information to a block page to show whether the blocked request was filtered on premise or in the cloud. This property returns a true value when McAfee WGCS filters and blocks the request.

In this task, you edit the default block page template named URL Blocked. The default template includes the title Blocked by URL Filter Database and the following standard text. Actual values for the properties in the template are written to the block page when it is generated.

<table>
<thead>
<tr>
<th>Your requested URL has been blocked by the URL Filter database module of McAfee Web Gateway. The URL is listed in categories that are not allowed by your administrator at this time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL:</strong></td>
</tr>
<tr>
<td><strong>URL Categories:</strong></td>
</tr>
<tr>
<td><strong>Reputation:</strong></td>
</tr>
<tr>
<td><strong>Media Type:</strong></td>
</tr>
</tbody>
</table>

In the following steps, you add a line to the block page after Media Type using the suggested text or custom text that you specify.
**Task**

1. In the Web Gateway interface, select **Policy | Templates**.
2. Expand the template folders **Default Schema | URL Blocked | en**.
3. Click **html**.

   The **HTML Editor** opens and displays the contents of the URLBlocked.html file.

4. In the file, locate the line that begins: `<b>Media Type: </b>`.
5. Immediately following this line, add these lines:

   ```html
   <b>Filter: </b>
   <script type="text/javascript">
   if ($InTheCloud$) {
       writeToDocument("McAfee Web Gateway Cloud Service");
   } else {
       writeToDocument("McAfee Web Gateway");
   }
   </script>
   ```

6. Click **Save Changes**.
7. To view the output, click **Preview**.

   The preview opens in a new tab. A line labeled **Filter** is added after the line labeled **Media Type**.

   To view the text in the preview that is written to the block page when it is generated, you can replace the property ($InTheCloud$) with the value (true) or (false). Click **Save Changes**, then click **Preview**. Depending on the value of **InTheCloud**, one of these lines is displayed.

   **Filter**: McAfee Web Gateway Cloud Service
   
   **Filter**: McAfee Web Gateway
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
- Logging
- Error handling
- Performance measurement
- Event monitoring with SNMP
- Transferring data for McAfee ePO monitoring
- Best practice: Monitoring file system usage
- Best practices - Sending access log data to a syslog server
- Best practice: Implementing TLS-secured usage of syslog data
- Sending syslog data to McAfee Enterprise Security Manager

**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

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

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

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>Provides basic appliance information.</td>
</tr>
<tr>
<td>• Name</td>
<td>Specifies the name of an appliance.</td>
</tr>
<tr>
<td>Performance</td>
<td>Provides key performance parameters.</td>
</tr>
</tbody>
</table>
| • Alert peaks, last 7 days | Indicates the 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 | Provides a 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. |
| McAfee Anti-Malware Versions | Provides update and version information on modules used in virus and malware filtering.  
  • Last update — Shows the number of minutes since the modules were last updated.  
  • Gateway Engine — Shows the version number of the McAfee Web Gateway Anti-Malware engine.  
  • Proactive Database — Shows the version number of the Proactive Database.  
  • DATs — Shows the version number of the DAT files (containing virus signatures). |
| URL Filter      | Provides update and version information for the module used in URL filtering.  
  • Last update — Shows the number of days since the module was last updated.  
  • Version — Shows the version number of the module. |
| Vulnerabilities | Provides information about recently detected CVE vulnerabilities and measures for mitigation.                                                                                                                      |

### 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.
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 rule set is available after the initial setup of an appliance. This rule set includes the following nested rule sets by default.

- **Access Log** — Contains a rule that writes entries about access to a Web Gateway appliance into the log
- **Access Denied Log** — Contains a rule that writes entries about attempts to access a Web Gateway appliance that were denied into the log
- **Found Viruses Log** — Contains a rule that writes entries about viruses that were found when requests were processed on a Web Gateway appliance into the log

To these default rule sets, you can add rule sets that you import from the rule set library, for example, the **Proxy Error Log** rule set. These rule sets are located in the **Logging** rule set group of the library.

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.
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.
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 437**
  
  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 438**
  
  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**.
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.

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**
2. From the Rule Sets menu, select Log Handler.
3 Click Add above the log handler tree, and from the drop-down list 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

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antimalware.Infected equals true</td>
<td>Continue</td>
<td>Set User-Defined.LogLine =</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ DateTime.ToWebReporterString</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ Authentication.Username</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ String.ReplaceIf Equals (IP.ToString(Client.IP), &quot;&quot;, &quot;,&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ ListOfString.ToString (Antimalware.VirusNames)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+ &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FileSystemLogging.WriteLogEntry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(User-Defined.logLine)&lt;Found Viruses Log&gt;</td>
</tr>
</tbody>
</table>

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 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

**Best practices - Adding a log file field**

Adding a log file field to the entries that are written in the log files of a log allows you to record additional information about activities that are performed on Web Gateway.

When you add a log file field, you might also want to adapt the log header and configure an entry for the new log file field. This way you ensure that the header, which is written into every log file, also includes information on this field.

**Add a log file field**

To add a log file field to an entry for a log file, append an appropriate element to the configuration for writing log file entries.

In this sample procedure, the destination IP address of a client request that is received on Web Gateway is added to the rule for writing log file entries into the default access log.

**Task**

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

2. Select **Log Handler**, expand the **Default** rule set on the log handler tree, and select **Access Log**.

3. Add an element for writing log file entries.
   
   a. Select the **Write access log** rule and click **Edit** immediately above.

   b. Select **Events**, then select the event **Set User-Defined.logLine** and click **Edit**.

   c. Under *To concatenation of these strings*, click **Add**.

   d. Click **Parameter property**, select **IP.ToString** from the properties list, and click **Parameters** next to the property name.

   To search for the property, you can type a suitable combination of characters in the filter field above the list, for example, *ip.tos*.

   The **Parameters For Property** window opens.
Click Parameter property and select URL.Destination.IP.

Click OK in the Parameters For Property window, then in the Enter a String window.

The new element appears in the Edit Set Property window, behind the last of the old elements, as shown here:

```
+ Number.ToString(Block.ID)
+ """
+ Application.ToString(Application.Name)
+ ""
+ IP.ToString(URL.Destination.IP)
```

4 Insert a delimiter to let the new log file field be separated from the preceding.

a Select the line with the three double quotes and click Edit.

b Enter a blank next to the double quote that appears in the window, then click OK.

The Enter a String window closes. In the Edit Set Property window, the line between the two elements should now look like this:

```
+ Application.ToString(Application.Name)
+ """
+ IP.ToString(URL.Destination.IP)
```

c Click OK in the Enter a string and Edit Set Property windows, then click Finish in the Edit Rule window.

5 Click Finish in the Edit Rule window, then click Save Changes.

Adapt the log header
Adapt the access log header by adding a header entry for the new element that you appended to the elements for log file writing.

Task
1 Select Policy | Settings.

2 On the settings tree, expand File System Logging and select the Access Log Configuration settings.

3 Under File System Logging Settings, make sure Enable header writing is selected, and at the end of the text string in the Log header field leave a blank after the last element and type server_ip.

   Header field names, such as server_ip, must not include blanks inside them, so always use underscores.

4 Click Save Changes.

Best practices - Creating a log
Creating a log allows you to log particular activities that are performed on Web Gateway.
For example, you want to log all requests that were sent from a particular client and were either invalid or blocked.
The logging is performed by a logging rule. This rule applies when a request of the kind that you want to log is received on Web Gateway. It does the following:

- Record information about the request in a log file entry (also known as log line)
  This entry can include the time when a request was sent, the name of the user who sent it, and other information.
- Write the entry into a log file
  Log files are stored in a log. To avoid excessive memory consumption, log files can be rotated and deleted after some time.

Like any other rule on Web Gateway, the logging rule must be contained in a rule set, which is termed a log rule set.

So creating a log that logs what you want to record includes the following activities:

- Creating a log rule set
- Creating a logging rule

To create the logging rule you need to configure:

- The rule criteria
- An event that builds log file entries
- An event that writes log file entries into a log file

When the write event is configured, the log that stores the log files is also specified.

### Configuring a log file entry

When creating a logging rule, you need to configure an event within this rule that builds the log file entries. A log file entry provides information about an activity that is performed on Web Gateway, for example, receiving and filtering a request.

Properties are used to store this information, for example, the Authentication.Username property is used to store the name of a user who sent a request.

To configure an event that builds log file entries, you need to specify all the properties you want to use for storing information. The event combines the values of these properties to the value of a single property, which is named `User-Defined.logLine`.

The value of the `User-Defined-logLine` property is then written by a write event into a log file.

When specifying the properties for the event that builds the log file entries, you need to consider some requirements.

### String format

A log file entry is a chain of data in string format. This means that the properties that are used for building an entry must have this format. Otherwise they need to be converted.

For example, to log a client IP address, the Client.IP property is used. The values of this property have a special IP address format, which can be converted using the `IP.ToString` property.
IP.ToString is specified as an element of the log file entry with Client.IP (in parentheses) as its parameter: IP.ToString(Client.IP). When this term is processed, it delivers a value that is an IP address in string format.

Empty elements
When a logging rule is processed, not all properties might be filled with values for a particular request. Accordingly, a log file entry can contain empty elements.

For example, the Authentication.Username property has no value if no authentication was performed for a user who sent a request. You can insert a placeholder, such as a dash, in this case.

The String.ReplaceIfEqual property is available for this purpose. It takes three parameters:

• The value that is actually recorded for a property
• A value to compare value 1 with
• A value to replace value 2 if 1 matches 2

For example, Authentication.Username, a blank, and a dash as parameters of the String.ReplaceIfEqual property, result in a dash for the user-name element of a log file entry if no user name is recorded.

Delimiters
To improve the readability of log file entries, configure delimiters between the elements of a log file entry. Delimiters can be blanks, quotes, and other characters.

Delimiters are specified in the same way as the main elements of an entry and are also interpreted as strings.

Create a log rule set with a logging rule
To create a logging rule that lets entries be written into log files and stored in a log, create a log rule set for it and configure rule criteria and events.

The purpose of the sample rule described here is to log all requests that are received from a client with a particular ID if the following also applies:

• A request is not valid under the HTTP protocol (response 403) or
• A request is blocked by the web security rules on Web Gateway (block ID is not 0)

Task
1 Select Policy | Rule Sets.
2 Select Log Handler and on the log handler tree, expand the Default log handler rule set.
3 Create a rule set for the logging rule.
   This rule set will be nested in the Default rule set.
   a Click Add, then Rule Set.
   b In the Name field, type a suitable name for the new log rule set, for example, Troubleshooting Log.
   c Click OK.
   The window closes and the new log rule set appears on the log handler tree.
4 Add a logging rule and name it.
   a On the settings pane, click Add Rule.
   b In the Name field, type a suitable name for the logging rule, for example, Log requests that caused issues.
Configure the rule criteria.

a Select Rule Criteria, then click Add and select Advanced Criteria.

b Select Client.IP as the property, equals as the operator, and in the field below Compare with, type an IP address as the operand, for example, 10.149.33.8.

c Click OK.

The Add Criteria window closes and the configured rule criteria appears in the Add Rule window.

d Click Add again for the second part of the criteria.

e In the same way as for the first part, configure Response.StatusCode, equals, and 403, then click OK.

f In the same way configure Block.ID, does not equal, and 0, then click OK.

Configure the event that builds the log file entry.

a Select Events and click Add, then select Set Property Value.

b From the properties list, select User-Defined.logLine and below To concatenation of these strings click Add.

c Click Parameter property and from the properties list, select DateTime.ToWebReporterString, as the first element of the log file entry. Then click OK.

The Enter a String window closes and the configured element appears in the Add Set Property window.

d Click Add, make sure Parameter value is selected, and type a blank followed by a double quote. Then click OK.

The Enter a String window closes and the configured delimiters appear in the Add Set Property window.

e Add the next element of the log file entry.

• Click Add, then Parameter property.

• Select String.ReplaceIfEquals and click Parameters next to the property name.

The Parameters For Property window opens.

• For the first parameter, click Parameter property, and select Authentication.Username.

• Select the second parameter and do not enter anything in the input field on the right.

This creates a blank as the parameter value.

• Select the third parameter and type a dash in the input field.

• Click OK in the Parameters For Property, then in the Enter a String window.

The element appears in the Add Set Property window.

f Click Add and type a double quote, a blank, and a double quote. Then click OK.

The Enter a String window closes and the configured delimiters appear in the Add Set Property window.
g Add the remaining elements by selecting the properties listed in the following. Insert delimiters between the elements, as shown in substep f.

- **Client.IP**
  
  For this element, configure the `IP.ToString` property with the `Client.IP` property as its parameter.
  
  Add the parameter as shown in substep e.

- **Request.Header.First.Line**

- **Header.Request.Get**
  
  Configure a parameter for this element by typing `user-agent` as the parameter value.

- **Rules.CurrentRuleSet.Name**

- **Rules.CurrentRule.Name**

- **Block.ID**
  
  For this element, configure the `Number.ToString` property with the `Block.ID` property as its parameter.

- **Block.Reason**
  
  After this last element, only use one double quote as the delimiter.

h Click **OK** to close the **Add Set Property** window.

The event that creates the log file entry appears in the **Add Rule** window.

It should look like this:

```csharp
Set User-Defined.logLine = 
  DateTime.ToWebReporterString 
  + " " 
  + String.ReplaceIfEquals 
  (Authentication.UserName, ",", "-") 
  + " " 
  + IP.ToString(Client.IP) 
  + " " 
  + Request.Header.First.Line 
  + " " 
  + Header.Request.Get("user-agent") 
  + " " 
  + Rules.CurrentRuleSet.Name 
  + " " 
  + Rules.CurrentRule.Name 
  + " " 
  + Number.ToString(Block.ID) 
  + " " 
  + Block.Reason 
  + ""
```

If you need to make changes, select the event, click **Edit**, and work with the **Edit Set Property** window.

In the representation of the event, the + symbols are added by the program.

Double quotes before and after a string value are also added. So, for example, the " " for the first delimiter represents a blank and a double quote.
7 Configure the event that writes the log file entries into a log file.
   a Under Events in the Add Rule window (or Edit Rule window if you made changes), click Add and select Event.
   b From the events list, select FileSystemLogging.WriteLogEntry and click Parameters.
   c Click Parameter property and from the list below, select User-Defined.logLine, then click OK.

   The Parameters for Execute Action window closes.
   d In the Add Event window, click Add below the Settings field.
   e Create new settings.
   These settings will be used by the File System Logging module (or engine) to handle the new log you are creating.
   • In the Name field, type a suitable name for the new settings, for example, Troubleshooting Log Settings.
   • Under Name of the log, type troubleshooting.log.
   • Select Enable header writing and in the Log header field, type the elements of the log header.
   The log header will appear at the beginning of every log file in the new log. It should represent the elements of the log file entry that you configured in step 6.
   So the log header might look like this:
   ```
   time_stamp "auth_user" "src_ip" "req_line" "user_agent" "rule_set" "rule"
   "block_page_res"
   "block_res"
   ```
   • Under Settings for Rotation, Pushing, and Deletion configure the following.
   • Select Enable specific settings for user-defined log.
   • Under Auto-Rotation, select GZIP log files after rotation to save memory space.
   • Configure the remaining settings under Auto-Rotation and those under Auto-Deletion as needed.

   Do not enable and configure the Auto-Pushing settings, as the log files for this new log are not pushed anywhere.
   f Click OK in the Add Settings window, then in the Add Event window.
   The windows close and the event that writes the log file entries appears in the Add Rule (or Edit Rule) window.
   g Click Finish.
   The window closes and the new logging rule appears as a rule of the Troubleshooting Log rule set on the Rule Sets tab.

You have now created a logging rule for recording a particular kind of requests.

The log files can be viewed in the log with the configured name. The log is accessible from the Troubleshooting top-level menu on the appliance you have configured the rule on.

The path to the log is Log files | user-defined logs.
Access log rule set
The Access Log rule set is a nested rule set in the Default Log Handler rule set.

<table>
<thead>
<tr>
<th>Nested default rule set – Access Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Write access.log**
*Always* -> Continue —
Set User-Defined.logLine = DateTime.ToWebReporterString + “ ...”
FileSystemLogging.WriteByteLogEntry (User-Defined.logLine)

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”)*
- 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.

<table>
<thead>
<tr>
<th>Nested default rule set – Found Viruses Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Write found viruses.log**
*Antimalware.Infected equals true* -> Continue —
Set User-Defined.logLine = DateTime.ToWebReporterString + “ ...”
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), "", ",")`
- 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**  
`Error.ID equals 14000`  

**Action**  
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.

Best practices - Working with the Error Handler
Working with the rules in the Error Handler rule sets gives you control over what happens when errors occur with processing web traffic on Web Gateway.
There are two main strategies of responding to errors:

• Fail-closed — When an error occurs, the request that a user sent to the web and that is being processed on Web Gateway is not allowed to proceed. A block message is shown to the user.

   This strategy is the default for error handling on Web Gateway.

• Fail-open — When an error occurs, the request that a user sent to the web and that is being processed on Web Gateway is allowed to proceed.

   In addition to this, logging activities and notifications can be triggered.

   This strategy is widely used within the web security policies of enterprise organizations.

The following are benefits of adopting a fail-open strategy for your network:

• Prevents business interruptions, as unimpeded web access is one of the most critical aspects for many jobs today.

• Avoids unnecessary calls to help desks, as you might consider it sufficient if the Web Gateway administrator is aware and can fix the problem. There is no need then to alert users.

A fail-open strategy can also be appropriate if failed components are compensated within your network while internal alerts are triggered and action is taken.
The flexibility of the Error Handler allows you to create rules to implement the main strategies in various ways, for example, as follows:

- **Strict fail-closed strategy on all errors**
- **Broad fail-open strategy to prevent any user impact**
- **Notifications to the Web Gateway administrator as part of a fail-closed or fail-open strategy**
- **Exceptions for requests from particular users and clients**

For example, a fail-open strategy is configured for executives and a fail-closed strategy for other users.

The default rule set for error handling includes the *Block on All Errors* rule set. This nested rule set is placed at the end of the default rule set. It blocks requests in all error situations that are not covered by the other nested rule sets.

When you configure a fail-open rule, make sure that this rule set is disabled or the rule set with the fail-open rule is placed before it.

**Configure a general fail-open strategy**

Configure a general fail-open strategy to let processing continue after any processing error that occurs.

**Task**

2. Select Error Handler and expand the Default error handling rule set.
3. For all rules in the nested rule sets:
   a. Select a rule and click Edit for this rule.
   b. In the Edit Rule window, select Action, then select Continue as the rule action.
   c. Click Finish.
4. Click Save Changes.

Processing of requests that users send to the web now continues on Web Gateway even when errors occur.

**Configure a fail-open strategy with a notification**

Configure a fail-open strategy with a notification to notify the administrator or another recipient when a particular error has occurred.

For the notification, you add an event to a rule that handles a particular error.

**Task**

1. Locate an existing rule:
   b. Select Error Handler and expand the Default error handling rule set.
   c. Select a nested rule set, for example, *Block on Anti-Malware Engine Errors*. Then select one of its rules, for example, *Block if anti-malware engine is overloaded*, and click Edit for this rule.
2. In the Edit Rule window, select Action, then select Stop Rule Set as the rule action instead of Block.
3 Configure an event for notifying someone:
   a Select Events and click Add.
   b Select Event, then select Email.Send and click Parameters
   c Type values for the three string parameters, for example, as follows:
      • Recipient (an email address): anyrecipient@samplecompany.com
         To configure more recipients, add their email addresses, separated by semicolons.
      • Subject (message name): Anti-Malware Overload
      • Body (message text): The anti-malware engines are overloaded, please inspect the
        mwg-antimalware-errors-log for more information.
   d Click OK twice, then click Finish.

4 Click Save Changes.

When the error that is handled by this rule occurs, a notification is sent to the configured recipient. You can also configure multiple notification events for different recipients with varying message texts.

Make sure that the Block on All Errors set is disabled or the rule set with the fail-open rule is placed before it.

Configure a fail-open strategy for user groups

Configure a fail-open strategy with a notification that is only sent for errors with processing requests from users belonging to a particular user group.

Task

1 Locate the rule that you configured a fail-open strategy with a notification for:
   a Select Policy | Rule Sets.
   b Select Error Handler and expand the Default error handling rule set.
   c Select the Block on Anti-Malware Engine Errors nested rule set, then select the Block if anti-malware engine is overloaded rule and click Edit for this rule.

2 Configure an additional part for the rule criteria:
   a In the Edit Rule window, select Rule Criteria, then select the criteria of the rule and click Add.
   b Select User/Group criteria, then select:
      • Authentication.UserGroups as the property
      • at least one in list as the operator
   c At the bottom of the right column, click Add List of String to add a list of user groups, and in the Add List window:
      • Name the list Groups to bypass on anti-malware overloads, then click OK.
      • Click Edit List and under List content, add the following string to the list (without quotes): Executives, then click OK twice.
   d In the Edit Rule window, select AND as the Boolean operator for this additional criteria part, then click Finish.
3 Click **Save Changes**.

When the error that is handled by this rule occurs, processing continues and a notification is sent to the configured recipient. It is only sent, however, if a user from the configured user group submitted the request that was processed when the error occurred.

Make sure that the **Block on All Errors** set is disabled or the rule set with the fail-open rule is placed before it.

**Default error handler rule set**

The Default error handler rule set is the default rule set for error handling.

<table>
<thead>
<tr>
<th>Default error handler rule set – Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Long Running Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Error.ID equals 20000</em></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Check Cache Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Statistics.Counter.GetCurrent(&quot;WebCacheDiskUsage&quot;)&lt;Default&gt; greater than or equals 95</td>
</tr>
</tbody>
</table>

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 =

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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Check Request Overload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Statistics.Counter.GetCurrent(&quot;HttpRequests&quot;)&lt;Default&gt; greater than or equals 480000</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Log File Manager Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Incident.ID greater than or equals 501 AND Incident ID less than or equals 600</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Handle Update Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Incident.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</td>
</tr>
</tbody>
</table>

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 that 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.OriginName
+ "; 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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Handle License Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Incident.ID equals 200</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Block on Anti-Malware Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Block on URL Filter Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Error.ID greater than or equals</em> 15000 AND <em>Error.ID less than or equals</em> 15999</td>
</tr>
</tbody>
</table>
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 equals 15005 –> 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.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Block on All Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
</tbody>
</table>

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 an 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.GetMillis` property records this time in milliseconds, the `Stopwatch.GetMicroSecs` 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.
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.HandleConnectToServer` for measuring the time needed to connect to external servers or `Timer.TimeConsumedByRuleEngine` 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Start stopwatch for rule set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Action</td>
</tr>
<tr>
<td><em>Always</em></td>
<td>-&gt; Continue</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Allow URLs in URL Whitelist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Action</td>
</tr>
<tr>
<td><em>URL matches in URL Whitelist</em></td>
<td>-&gt; Continue</td>
</tr>
</tbody>
</table>

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")`.

---

**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_.

---

**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**.

**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.

<table>
<thead>
<tr>
<th>Library rule set – Bypass ePO Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <code>Command.Name equals “CONNECT”</code></td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

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.
Best practice: Monitoring file system usage

It is important to monitor file system usage in the /opt partition on Web Gateway, as this partition is used for storing system files while the appliance software is also installed there. This means that a full opt partition impacts the performance of the appliance.

The /opt partition can be monitored based on the following:

- **Incident ID** — An incident with ID 22 is generated on Web Gateway when the /opt partition is filled up to a level of 90%. This incident triggers an alert on the dashboard.
  
  The utilization level that leads to generating the incident is fixed and cannot be configured.

- **Statistical counter** — A statistical counter called FileSystemUsage is available on Web Gateway to record utilization of the opt partition.
  
  Using this statistical counter in a suitable rule, you can configure your own utilization threshold to trigger various kinds of alerts and log entries.

**Working with a statistical counter**

The statistical counter that you work with to monitor the /opt partition is configured as the criteria of a rule set. For example, if the statistical counter records an 85% utilization of the /opt partition, the rules in the rule set are processed.

The rule set is filled with the following:

- A rule that creates a notification message, for example, "/opt partition usage is at 85 %".
- Several rules that send or log this message

Place the rule set as an embedded rule set in the Monitoring rule set, which is by default provided among the rule sets of the Error Handler log on Web Gateway.

The Monitoring rule set and its embedded rule sets are processed every minute by the error handler on Web Gateway, due to the use of incident ID 5 in the criteria of the embedding rule set.

In accordance with the names of the embedded monitoring rule sets that are by default available, your rule set for monitoring the /opt partition might be named Check Opt Partition.

Depending on the threshold that you choose, the criteria for this rule set reads as follows:

**StatisticCounter.GetCurrent ("FileSystemUsage") greater than or equals 85**

**Rules in a rule set for monitoring the /opt partition**

A rule set for monitoring the /opt partition can be filled with the rules shown in the following.

This rule creates the notification message that is sent or logged by the other rules in the rule set.

<table>
<thead>
<tr>
<th>Name</th>
<th>Create notification message</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Always

---> Continue

Set User-Defined.notificationMessage = "/opt partition usage at:
+ Number.ToString
(Statistics.Counter.GetCurrent ("FileSystemUsage")<Default>)
+ "%"

These rules use the notification message to perform the following activities:

• Send an SNMP trap
• Create a syslog entry
• Send an email notification
• Write a log file entry

<table>
<thead>
<tr>
<th>Name and criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send SNMP trap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Send SNMP trap

Always

---> Continue

Set SNMP.Trap.Additional = User-Defined.notificationMessage

SNMP.Trap.Send.User (12, "High /opt partition utilization detected.")

Create syslog entry

Always

---> Continue

Syslog (3, User-Defined.notificationMessage)

Send email for notification

Always

Continue

Email.Send ("Enter valid email", "Message from McAfee Web Gateway, User-Defined.notificationMessage) <Monitoring>

Write /opt partition into log

Always

---> Continue

+ User-Defined.notificationMessage) <Monitoring>

FileSystemLogging.WriteLogEntry (User.Defined.monitorLogMessage <Monitoring
Incident Log>
Troubleshooting issues with file system usage

You can identify the reasons for issues with file system usage and take measures to prevent these issues.

Identify issues with file system usage

To identify issues with file system usage, you can search the /opt partition for large directories.

Task

1. Log on to the appliance that you want to identify issues on from a local system console, or remotely using SSH.

2. Run the following commands:

```
  df -h
  du /opt -Dm | sort -n | tail
```

A search is started for the largest folders in the /opt partition. The results are output in ascending order of size, for example, as follows.

<table>
<thead>
<tr>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1158</td>
<td>/opt/mwg/plugin/data</td>
</tr>
<tr>
<td>1320</td>
<td>/opt/mwg/plugin</td>
</tr>
<tr>
<td>5010</td>
<td>/opt/mwg/storage/default</td>
</tr>
<tr>
<td>6011</td>
<td>/opt/mwg/storage</td>
</tr>
<tr>
<td>7937</td>
<td>/opt/mwg/log/debug/cores</td>
</tr>
</tbody>
</table>

3. If you cannot determine the source of an issue, create a listing for support, using the following commands:

```
  df -h
  du /opt -Dm | sort -n > opt_directory_listing.txt
```

The command outputs a .txt file with a listing of the directories in the /opt partition.

Preventing excessive utilization of the /opt partition

You can prevent excessive utilization of the /opt partition by taking appropriate measures regarding the files that are stored in this partition.

The following file types often cause the /opt partition to run out of space due to their sizes.

User-defined logs

User-defined logs are, for example, the access.log and access_denied.log. You can find these logs under /opt/mwg/log in the user-defined-logs directory and its subdirectories.

To prevent utilization issues due to log files, set up appropriate rotation, deletion, and push schedules, using the File System Logging settings.

Make sure that you also compress the log files after rotation using the GZIP log files after rotation setting.

Trace files

Trace files are, for example, created for connection or rule engine tracing. You can find these files under /opt/mwg/log/ in the debug directory and its subdirectories.

This directory also contains trace files for authentication, quota, PD storage, the log manager, and the Coordinator subsystem of the Web Gateway appliance.
To prevent utilization issues due to trace files, create them only just before your testing or troubleshooting activities and stop tracing immediately after completing these activities. Many tracing options also allow you to restrict the tracing to individual IP addresses.

**Best practice:** Connection tracing files are by default removed when the appliance is restarted. Do not wait for a restart and manually remove these files as soon as possible.

**Temporary files**
Temporary files are found under `/opt/mwg/` in the temp directory.

Web Gateway usually creates temporary mwg-core files in the temp directory while downloading and scanning files. These files are managed by the mwg-core process and are removed after the download and scanning has completed.

**Best practice:** Streaming Media files that are scanned for anti-malware filtering can cause very large temp files, as streams have no known end. Let these files bypass scanning.

**Support files**
Support might request you to provide additional troubleshooting files for reviewing, for example, files that you find under `/opt/mwg/log` in the debug directory. These files include tcpdump, feedback, and core files, as well as some others.

After support has confirmed the receipt of these files, you can remove them from the `/opt` partition.

### Best practices - Sending access log data to a syslog server

You can configure Web Gateway to send data that is recorded in the access log to a syslog server.

Data about requests for web access that Web Gateway receives from its clients is recorded in the access log. The recording is performed by a rule in a rule set for log handling, which is enabled by default. By adding another rule this data can be made available to a daemon, which sends it to a particular syslog server.

The recorded data includes date and time of a request, the user name of the user who sent the request, the requested URL, and other information. You can modify the configuration to record more or different information about web access.

The data can be sent under different protocols and in different formats. You can also configure a severity level to send, for example, only data about emergencies.

To send the data, you must complete the following:

- Add a rule that makes access log data available to the syslog daemon.
- Adapt the `rsylog.conf` system file to let the daemon send data to a syslog server.

These activities must be completed on every Web Gateway appliance that access log data are to be sent from. In a similar way, you can also configure the sending of other log data.

### Protocols for sending data
Data can be sent to a syslog server under the UDP or TCP protocol. Some syslog servers have no TCP listener ports, however. The most common UDP listener port is 514, whereas under TCP the port varies from application to application.
Data formats

Data is sent to syslog servers in different formats, depending on the server type. If in doubt, ask the administrator who is responsible for the syslog server.

- **Default format** — The default log handling rule uses this format to record access log data.
  
The format and modified versions of it are also accepted by McAfee Content Security Reporter, version 2.0.

- **SIEM (Nitro) format** — This format is required if the syslog server is provided by McAfee® Enterprise Security Manager (McAfee ESM) (SIEM, formerly known as Nitro).
  
You can import the SIEM Nitro Integration rule set from the online rule set library. This rule set contains a rule that uses the SIEM (Nitro) format to record access log data.

- **CEF format** — This format is required if the syslog server is provided by an ArcSight security manager or a similar program.
  
You can import the CEF Syslog rule set from the online rule set library. This rule set contains a rule that uses the CEF format to record access log data.

Severity levels

Data with differing severity can be sent to a syslog server. The severity levels are listed in the following. Severity level 6 is recommended.

- 0: Emergency (emerg) — System unusable
- 1: Alert (alert) — Action to be taken immediately
- 2: Critical (critical) — Critical condition
- 3: Error (error) — Error condition
- 4: Warning (warning) — Warning condition
- 5: Notice (notice) — Normal, but significant condition
- 6: Information (info) — Informational message
- 7: Debug (debug) — Message for debugging

Add a rule for sending access log data

To send access log data from Web Gateway to a syslog server, add a rule to the rule for recording data in the Access Log rule set.

**Task**

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

2. Click **Log Handler**, expand the **Default** rule set, and select the nested **Access Log** rule set.

   The content of the nested rule set appears on the configuration pane. By default the rule set contains a rule that writes data about web access to a log line.
Add the following rule to make access log data available to the daemon that sends it to the syslog server.

Name

Make access log data available to syslog daemon

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt;</td>
<td>Continue</td>
</tr>
</tbody>
</table>

The rule uses an event to make the access data that has been written to a user-defined log line before to the syslog daemon. The syslog daemon sends it to the syslog server. The daemon is configured in the `rsyslog.conf` system file.

The first event parameter specifies the severity level of the access log data.

Click **Save Changes**.

The rule is for making available data that the preceding rule records in default format. If the syslog server requires a different format, replace the preceding rule with a rule that uses the required format.

You can import rule sets with rules that write data in SIEM or CEF format from the online rule set library.

Adapt the `rsyslog.conf` system file for sending access log data

Adapt the `rsyslog.conf` system file to ensure that access log data is successfully sent to a syslog server.

Work with the **File Editor** on the user interface of Web Gateway to adapt the system file. If you use commands from a system console, your changes will be overwritten by future updates.

**Task**

1. Select **Configuration** | **File Editor**.

2. On the files tree, select **rsyslog.conf**.

3. Edit the file to adapt it for sending access log data.

   a. Look for the following line:

   ```
   *.info;mail.none;authpriv.none;cron.none                /var/log/messages
   ```

   The line is part of a section on rules.

   ```
   # Include config files in /etc/rsyslog.d
   $IncludeConfig /etc/rsyslog.d/*.conf
   ###RULES###
   # 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
   ```
b Replace mail with daemon in this line and insert a - (dash) before the path information.

```
*.info;daemon.none;authpriv.none;cron.none    -/var/log/messages
```

This modification prevents the syslog daemon from sending data to the `var/log/messages` partition on the disk of the Web Gateway appliance system.

The info before daemon specifies the severity level of the data.

You can now direct the data to the intended destination.

c To send data to a syslog server under the UDP protocol, insert:

```
daemon.info.@x.x.x.x:514
```

x.x.x.x must be substituted with the IP address of the syslog server.

To send messages to a syslog server under TCP, insert:

```
daemon.info.@@x.x.x.x:<port number>
```

4 Click Save Changes.

### Resolving issues with sending access log data

Several measures can be taken to resolve issues with sending access log data from Web Gateway to a syslog server.

- If access log data is not received on the syslog server, it might still be written to the `var/log/messages` partition on the disk of the Web Gateway appliance system.

  Run the following command from a system console to verify that data is not written to disk:

  ```
tail -f /var/log/messages
  ```

- If access log data is not received on the syslog server, it might be due to restrictions that are, for example, imposed by a firewall. You can perform a tcpdump to see whether Web Gateway sends data packets to the syslog server at all.

  Run the following command from a system console to see the data packets, for example, when they are sent to the syslog server under the UDP protocol:

  ```
tcpdump port 514
  ```

  You should also review the rsyslog.conf system file to make sure that sending data to the syslog server is configured correctly.

- Web Gateway truncates a data packet that is sent to the syslog server by default if it has more than 2000 characters.

  Add the following line to the rsyslog.conf system file to adjust the packet length:

  ```
$MaxMessageSize <maximum number of characters>
```
Best practice: Implementing TLS-secured usage of syslog data

You can implement use of the TLS protocol that is provided by an rsyslog package for TLS-secured sending of messages with syslog data.

The `rsyslog-gnutls` package and several related packages are installed by default on the Web Gateway appliance system. The rsyslog-gnutls package provides the TLS protocol, which allows you implement TLS encryption for secure sending of log messages from a syslog client to a remote syslog (rsyslog) server.

TLS-secured sending of syslog messages requires the use of SSL certificates for the server and its clients, as well as for a root certificate authority (root CA) that signs these certificates.

The packages that are involved in implementing TLS encryption include:

- `rsyslog-gnutls-5.8.10`
- `rsyslog-5.8.10`
- `gnutls-2.8.5`

For more information about these packages, see the documentation of the vendor who provides them (RSYSLOG).

High-level steps for implementing TLS-secured usage of syslog data

To implement TLS-secured usage of syslog data with the rsyslog-gnutls package, complete the following high-level steps.

Task

1. Make sure the system time and date is the same on the appliance that you plan to configure as the syslog server and its clients.

   The system that you use for creating certificates on must also have the same time and date.

2. Create certificates for a root CA, as well as for the syslog server and its clients.

3. Configure a syslog server.

4. Configure one or more syslog clients.

5. Send test messages from the syslog clients to the syslog server.

Prepare the use of TLS-secured syslog data

Make sure that system time and date is the same on all appliances that you want to prepare the use of TLS-secured syslog data on and create certificates for the TLS encryption.

Task

1. Log on to a Web Gateway appliance that you want to prepare the use of TLS-secured data on from a local system console or remotely using SSH.

2. [Optional] If a version of the rsyslog-gnutls package is already installed on an appliance, you can run the following command to identify this version.

   ```
   rpm -qa rsyslog-gnutls
   ```
3 Set system time and date on this appliance and on all other appliances that you want to prepare for sending and receiving TLS-secured syslog messages. Set time and date also on the system that you use to create certificates.

On Linux systems, you can run the following command.

```
date <mm for the month><dd for the day><hh for the hour, using the 24-hours system><mm for the minute><yy for the year>
```

For example, to set system time and date to November, 20th, 2016, 9:45 p.m., run:

```
date 1120214516
```

On Linux systems, you can also synchronize the time and date on the mainboard of the hardware platform for the appliance with that of the appliance software. For this synchronization run:

```
hwclock -systohc
```

4 Create and store certificates for the root certificate authority (CA) and the appliances that send and receive TLS-secured syslog messages.

   a Use a certificate creation tool, for example, OpenSSL or Certtool, to create the certificates. For more information, see the documentation of the vendor who provides the rsyslog package (RSYSLOG).

   b Log on to the appliance that you want to store the certificates on from a local system console or remotely with SSH.

   c Run the following command to create a directory for storing the certificates.

      ```
      mkdir -pv /etc/rsyslog.d/cert
      ```

   d Copy the certificates to the directory. Run, for example:

      ```
      cp ca.pem syslogserver.cert.pem syslogserver.key.pem syslogclient1.cert.pem syslogclient1.key.pem syslogclient2.cert.pem syslogclient2.key.pem /etc/rsyslog.d/cert
      ```

   e [Optional] Check the content of the certificates. Run, for example:

      ```
      openssl x509 -in syslogclient1cert.pem -text noout|less
      openssl x509 -in syslogclient1cert.der -inform der -text noout
      ```

**Configure a syslog server to receive TLS-secured data**

Work with a rsyslog system file on a Web Gateway appliance to configure a syslog server that receives TLS-secured data.

**Task**

1 On the user interface, select **Configuration | File Editor**.

2 On the appliances tree, select the appliance that you want to configure a syslog server on, then select **rsyslog.conf**.

   The content of the system file appears in the configuration frame.
3 Add the following lines to the file content.

```
$ModLoad imtcp.so #Specifies the TCP listener that listens to requests sent from the clients.
$DefaultNetstreamDriver gtls #Requires use of the netstream driver.
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/cert/ca.pem #Specifies the root CA.
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/cert/server.cert.pem #Specifies the certificate for the server.
$DefaultNetstreamDriverKeyFile /etc/rsyslog.d/cert/server.key.pem #Specifies the certificate key for the server.
$InputTCPServerStreamDriverAuthMode x509/name
$InputTCPServerStreamDriverPermittedPeer <client IP address> #Specifies the client through its IP address.
$InputTCPServerStreamDriverMode 1 #Requires the server to run in TLS mode only.
$InputTCPServerRun 10514 #Specifies the listener port that the syslog communication starts at.
```

4 Log on to the appliance from a local system console or remotely using SSH.

5 Run the following command to restart the rsyslog function on the appliance.

```
/etc/init.d/rsyslog restart
```

After restarting rsyslog, a TLS-secured connection is set up, using the settings in the configuration file and the certificates.

6 Verify that the TLS-secured connection has been set up successfully.

```
cat /var/log/messages
```

After running the verification command, you should see messages like the following displayed.

```
Nov 15 11:23:37 testdev rsyslogd: [origin software="rsyslogd" swVersion="5.8.10" x-pid="41552" x-info="http://www.rsyslog.com"] start [root@testdev tls]
```

### Configure a syslog client to send TLS-secured data

Work with a rsyslog system file on a Web Gateway appliance to configure a syslog client that sends TLS-secured data.

**Task**

1. On the user interface, select Configuration | File Editor.

2. On the appliances tree, select the appliance that you want to configure a syslog client on, then select rsyslog.conf.

   The content of the system file appears in the configuration frame.
3 Add the following lines to the file content.

```bash
$template TEST-MESSAGE, "%HOSTNAME" ClientText: %syslogtag%%msg%
$WorkDirectory /var/spool/rsyslog #Specifies where to store spool files.
$ActionQueueFileName fwdRule1 #Provides a unique name prefix for spool files.
$ActionQueueMaxDiskSpace 1g     #Sets a space limit of 1 GB.
$ActionQueueSaveOnShutdown on   #Saves messages to disk upon shutdown.
$ActionQueueType LinkedList     #Lets the process run asynchronously.
$ActionResume RetryCount -1     #Triggers an unlimited number of retries if the server is down
$DefaultNetstreamDriver gtls   #Requires use of the netstream driver.
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/cert/ca.pem #Specifies the root CA.
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/cert/client.cert.pem #Specifies the certificate for the client.
$DefaultNetstreamDriverKeyFile /etc/rsyslog.d/cert/client.key.pem #Specifies the certificate key for the client.
$InputTCPServerStreamDriverAuthMode x509/name
$InputTCPServerStreamDriverPermittedPeer <server host name or IP address> #Specifies the server through its host name or IP address.
$InputTCPServerStreamDriverMode 1 #Requires the server to run in TLS mode only.
$InputTCPServerRun 10514 #Specifies the listener port that the syslog communication starts at.
```

4 Log on to the appliance from a local system console or remotely using SSH.

5 Run the following command to restart the rsyslog function on the appliance.

```
/etc/init.d/rsyslog restart
```

After restarting rsyslog, a TLS-secured connection is set up, using the settings in the configuration file and the certificates.

6 Verify that the TLS-secured connection has been set up successfully.

```
cat /var/log/messages
```

After running the verification command, you should see messages like the following displayed.

```
Nov 15 11:23:37 HyperVMlos2AD kernel: Kernel logging (proc) stopped.
Nov 15 11:23:37 HyperVMlos2AD rsyslogd: [origin software="rsyslogd" swVersion="5.8.10" x-pid="57261" x-info="http://www.rsyslog.com"] start
[root@HyperVMlos2AD rsyslog.d]
```

You can now send TLS-secured syslog messages. Run the following command to send a test message:

```
logger "TLS-secured test message"
```

---

**Sending syslog data to McAfee Enterprise Security Manager**

Data that is logged on Web Gateway in syslog log files can be sent to McAfee Enterprise Security Manager (McAfee ESM).

The data transfer is controlled by a rule in a rule set that is available in the online rule set library for Web Gateway. The component of McAfee ESM that the data is sent to is the McAfee SIEM Receiver.
To enable the transfer, you adapt a system file for remote use of syslog data on Web Gateway. The name of this system file is `rsyslog` (the `r` in the file name stands for `remote`). You must also configure the McAfee SIEM Receiver to let Web Gateway be included as a data source in the McAfee ESM environment.

Version 9.3.2 or a later version of McAfee ESM is required for the data transfer to work.

**Configure the sending of syslog data**

To send syslog data that is collected on Web Gateway to McAfee ESM, complete the following high-level steps.

**Task**

1. Import the McAfee SIEM rule set from the online rule set library for Web Gateway. Place it as a nested rule set in the default Log Handler rule set.
   
   In the online rule set library, this rule set is available under **SIEM (Nitro) Integration**.

2. In the imported rule set, enable the `Send to syslog` rule and disable the `Send to nitro.log` rule.

3. Use the File Editor to adapt the `rsyslog` system file for the data transfer.

   If you are running multiple Web Gateway appliances in a Central Management cluster, adapt the system file on every appliance within the cluster.

4. On McAfee ESM, configure the McAfee SIEM Receiver to let Web Gateway be included as a data source.

   For more information, see the documentation for McAfee ESM and the **Data Source Configuration Guide**. The guide is provided in the online rule set library under **SIEM (Nitro) Integration**.

**Adapt the rsyslog system file for the data transfer**

Adapt the `rsyslog` system file on Web Gateway to ensure that syslog data is successfully sent to McAfee ESM.

**Task**

1. Select **Configuration | File Editor**.

2. On the files tree, select `rsyslog.conf`.

   The file content appears on the configuration pane.
3 Edit the file to adapt it for the data transfer.

The edited file should look as shown in the following. The modified lines are in the paragraph that begins with: The below will direct all daemon.info messages to the remote syslog server ...

```
# default parameters
$DirCreateMode 0755
$FileCreateMode 0640
$FileGroup adm
$umask 0026

# Include config files in /etc/rsyslog.d
$IncludeConfig /etc/rsyslog.d/*.conf

# 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!

# The following directs all daemon.info messages to the remote syslog server at [IP_OF_MCAFEE_EVENT_RECEIVER]
# add @@ for TCP syslog for example
# daemon.info @192.168.1.1
*.info;daemon.!=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
```

4 Click Save Changes.

**Fine-tuning the collection and evaluation of syslog data**

Several fine-tuning activities can be performed to ensure that relevant syslog data is collected on Web Gateway and efficiently evaluated on McAfee ESM.

The amount of syslog data that is collected can be throttled by excluding less relevant data and restricting the process to logging only important events. Relevant data can also be added, however, to the syslog data by implementing additional logging activities.

On McAfee ESM, data aggregation can be disabled to ensure that no relevant data is overlooked.
Throttling the amount of syslog data

The amount of syslog data that Web Gateway sends to McAfee ESM can be throttled by taking, for example, the following measures.

- **Excluding Authentication Required (status code 407) responses** — These are standard responses that do not require much attention regarding web security.

  To exclude these responses from the syslog data that is transferred, add a rule in the rule set that you imported.

  The rule must be placed, together with other throttling rules that you might implement, at the top of the rule set. It should look as follows:

  **Name**
  
  **Exclude 407 responses**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response.StatusCode equals 407</td>
<td>=&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>

- **Sending only logged Block actions** — Block actions are crucial in maintaining web security, but usually account for only a small proportion of web traffic.

  To restrict the syslog data that is transferred to log files for these actions, add a rule in the rule set that you imported.

  The rule must be placed, together with other throttling rules that you might implement, at the top of the rule set. It should look as follows:

  **Name**
  
  **Send only logged Block actions**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block.ID equals 0</td>
<td>=&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>

Adding hashes of infected files to the syslog data

To the syslog data can be added the hash values of files that were processed on Web Gateway and found to be infected. File hashes can be useful for tracking infections and possible outbreaks.

As hashing consumes a large amount of resources, we recommend using it only for important issues. If in doubt, consult McAfee support.

To enable the calculation and logging of file hashes, add an event to the rule that detects and blocks infected files. By default, this rule is **Block if virus was found** in the Gateway Anti-Malware rule set.

The event should look as follows:

```plaintext
```

The **Header.Block.Add** event is a preconfigured event that you can select from the list of available events. It adds an entry to the syslog log when the rule that it is inserted in applies.
The event takes two parameters, which you must configure:

- **X-Hash-MD5** — Name of the log entry
- **Body.Hash("md5")** — Value of the log entry

This parameter is a property for calculating the hash value of a file. Here it calculates the hash value of the infected file that was sent to Web Gateway as the body of a request or response.

The property takes itself a parameter, which determines the method for calculating the hash.

If you are working with the key elements view for rule sets, you must switch to the complete rules view to add the event.

After adding the event, the blocking rule should look as follows.

<table>
<thead>
<tr>
<th>Name</th>
<th>Block if virus was found</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Action</td>
</tr>
</tbody>
</table>

### Disabling the aggregation of syslog data

When the McAfee SIEM Receiver receives syslog data from Web Gateway, this data is by default aggregated into a single record. While aggregation can be useful for many data sources, it could be undesirable for Web Gateway, as critical information might get lost during aggregation.

You can disable aggregation for Web Gateway data on McAfee ESM.

For more information, see the documentation for McAfee ESM and the *Data Source Configuration Guide*. The guide is provided in the online rule set library under *SIEM (Nitro) Integration*.

### Resolving issues with the transfer of syslog data

To resolve issues with sending syslog data from Web Gateway to McAfee ESM, several measures can be taken:

- Review the configuration on Web Gateway and make sure that the following applies:
  - The *Send syslog* rule is enabled.
  - The IP address of the McAfee SIEM Receiver is correctly specified in the `rsyslog` system file.
- Review the configuration on McAfee ESM.
  - For more information on this step and on others that are performed on McAfee ESM, see the documentation on McAfee ESM and the *Data Source Configuration Guide*. The guide is provided in the online rule set library under *SIEM (Nitro) Integration*.
  - Verify that syslog data is generated on Web Gateway, for example, by running the following command from a system console:

    ```
tcpdump -s 0 -I any port 514
```
• Verify that syslog data is received on the McAfee SIEM Receiver.
• Verify that the syslog log is generated on Web Gateway in proper format.

Entries in the syslog log usually look as follows:

```plaintext

McAfeeWG|time_stamp=[30/Mar/2014:05:18:20 +0000]|auth_user=|src_ip=172.18.19.225|server_ip=69.20.171.162|host=www.nitroguard.com|url_port=80|status_code=200|bytes_from_client=376|bytes_to_client=200|categories=|rep_level=|method=GET|url=http://www.nitroguard.com/ngdb.dll?NG:DoIt:0:Info=D8BC0B7C97D2C352AFE4643FEA44AE4D4C70F79271D462B64294729E046CB07B5458AC24BA31B061A12313E016EB7F62ED267DC6FE9A02A552681347EF796303514934EO08E0DA7E27F5EEA225B0DB74367AF4FEA574EA6137728|media_type=|application_name=|user_agent=Mozilla/4.0 (compatible; Synapse)|block_res=0|block_reason=|virus_name=|hash=|
```
Monitoring
Sending syslog data to McAfee Enterprise Security Manager
Several methods and tools are available for troubleshooting problems on an appliance.

Contents
- Troubleshooting methods
- Rule tracing
- Create a feedback file
- Enable the creation of core files
- Enable the creation of connection tracing files
- Create a packet tracing file
- Work with system and network tools
- Restart a service of the operating system
- Display running AV threads
- Back up and restore an appliance configuration
- Reset the appliance password

Troubleshooting methods

When problems arise on an appliance, you can use different methods to solve them.

Rule tracing

You can create and review rule traces on the user interface. The traces record how rules were processed to deal with requests sent from clients of Web Gateway, as well as with the responses to these requests that were received from the Web.

Reviewing these traces enables you to find out which rules were processed and what actions, for example, block actions, they executed for a particular request.

Tracing information is shown on the user interface for:
- Cycles — Request, response, or embedded objects cycle that a rule action was executed in
- Rules — Rules that were processed in these cycles
- Rule sets — Rule sets that these rules belong to
- Rule Criteria — Criteria that matched to let a rule action be executed
- Properties — Properties and the values they had when the rule criteria matched
- Actions — Actions that were executed when the rule criteria matched
- Events — Events that were executed when the rule criteria matched
Recording and inspecting 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 that went on before 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

Using 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.

Using system tools
You can use system tools to perform a service restart on Web Gateway and also to display the AV threads that are currently running.

Restoring 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.

Resetting the appliance password
Troubleshooting includes the option to reset the appliance password. This password is the root password that is required when accessing an appliance from a system console using the command line. This password is also known as root or console password.

Resetting this password may be required, for example, if you cannot remember it or look it up somewhere.

Rule tracing
To debug issues with rule processing, you can use rule tracing functions on the user interface.

Rule traces can be created, which record the activities that were completed to process the implemented rules when users of your network sent requests for web access from particular clients.

You can filter these traces according to the date of creation, the URL that was sent with a request, or the rule action, such as Block, Redirect, or Continue, and others, that was executed when a rule was processed.

Tracing covers all activities in the different processing cycles that were performed for a request, including the request, response, and embedded object cycles. Tracing results can be viewed separately for different cycles.
Properties in the criteria of the rules that were involved in the processing can also be viewed separately, together with the values they were set to when the rules were processed.

Three panes are provided on the rule tracing page of the user interface to let you complete rule tracing activities.

- **Traces pane** — Allows you to create traces, filter, and remove them
  
  You can also export and store traces and import them again for viewing later on or import traces that have been created on other Web Gateway appliances.

- **Rules pane** — Allows you to select a processing cycle and view the rule sets and individual rules that were processed in this cycle

- **Details pane** — Allows you to view the rule criteria of individual rules with their properties and the values the properties have been set to

**Cycles in rule tracing**

Processing starts when a request for web access has been received from a client of Web Gateway. It is performed in different cycles, beginning with the request cycle, in which rules are processed that are related to the elements of the request itself, for example, to a URL that was sent with a request.

If none of the rules in this cycle forbids a forwarding of the request to the web, for example, due to a negative categorization of a URL, the request is forwarded. Processing then waits for a response from the web.

When the response arrives, the rules of the response cycle are processed. For example, when a file that was requested for downloading is sent in response, it is scanned for virus and other malware infections according to a particular rule and eventually passed on or not to the client that requested the download.

Other processing cycles are performed for embedded objects sent with requests or responses. Processing activities can also be logged according to the configured logging rules.

All processing that is performed in the different cycles for an initial request from a client of Web Gateway can be viewed as an entity, which is termed a transaction.

To debug an issue with rule processing, you can analyze the complete rule trace of a transaction or focus on a particular cycle that seems interesting with regard to problem solving.

**Properties in rule tracing**

Whether a rule applies and executes a particular action, for example, a Block action that blocks a request for web access, depends on the rule criteria, which contains properties that are set to particular values during the processing.

For example, the Antimalware.Infected property, which is contained in the rule criteria of a default anti-malware rule, is set to true when a scanned web object has been found to be infected by viruses or other malware. Then the criteria of this rule matches, and a Block action is executed.

When analyzing a rule trace, it can be useful to look at the properties that were involved in rule processing and the values they were set to. Therefore, properties and their values can also be viewed separately.

**Deleting and restoring rule traces**

Rule traces can be removed from the panes of the rule tracing page, but not deleted on that page.

To delete rule traces, you need to access the Rule tracing files section, which is provided for every individual appliance under the Troubleshooting top-level menu.
In this section, you can also restore traces to the rule tracing panes that you have previously removed.

For each client IP address that is traced, up to 5000 traces can be stored on an appliance. When this number is exceeded, the oldest 100 traces are deleted.

The deletion is not reflected on the rule tracing panes, so you might see entries for traces that you cannot access because the traces have already been deleted.

Debug rule processing issues using rule tracing

Use the options of the rule tracing panes to create rule traces and review them to debug issues with rule processing.

Task
1  Select Troubleshooting.

2  On the troubleshooting tree, select Rule Tracing Central.

   The rule tracing panes appear.

3  Work with the rule tracing panes to debug rule processing issues.

Use rule tracing to find out why a request was blocked

When a request for web access that a user sent from a client of Web Gateway has been blocked, you can use rule tracing to find the rule that blocked the request and the reason why it was done.

This is a sample procedure that describes one of several ways to use rule tracing for recording and analyzing rule processing on Web Gateway.

Task
1  Select Troubleshooting and on the appliances tree, select Rule Tracing Central.

   The rule tracing panes appear.

2  Create rule traces.
   a  In the traces pane, leave the name of the current appliance, which appears in the appliances names field.

      In this sample procedure, you will perform rule tracing for requests that were processed on this appliance.

   b  In the client IP address field, enter the IP address of the client that sent the request you want to do rule tracing for.

   c  Click Go.

      Rule traces for the latest requests received from the client are created. When trace creation is completed, entries for the traces appear in the traces field.

3  Filter the rule traces.
   a  In the time and URL filtering field, enter the URL that was sent with the blocked request.

      The rule traces are filtered to show only entries for traces that were performed for requests to access a web object with this URL.

      Let us assume that a request with this URL was only submitted once by the client in question. This would mean only one entry is shown as the filtering result.
b  Select the entry.

Detailed information from the trace that recorded rule processing for the request with this URL is shown in the rules and details panes.

4  Review a rule trace.

a  Review the tracing information in the rules pane.

The rules that were processed to deal with the request are shown with their rule sets.

The rule that blocked the request is selected and marked by a red arrow. If the arrow points to the right, the rule blocked the request in the request cycle. If the arrow points to the left, it was in the response cycle.

b  Review the tracing information in the details pane.

• The cycle in which the rule blocked the request, the name of the rule, its criteria, action, and event are shown.

  The criteria is marked with a grey hook, which means it has matched.

• Under **Evaluated** in the field below the criteria with the hook, the criteria is repeated.

  Under **Value** in the same field the value is shown that the property had at the time when the criteria matched and the rule blocked the request.

Let us assume that, for example, the details pane shows the following details for the rule that blocked the request.

• **Cycle** — Response

• **Rule name** — Block if virus was found

• **Criteria** — Antimalware.Infected<Gateway Anti.Malware> equals true

• **Evaluated** — Antimalware.Infected equals true, **Value** — true

• **Action** — Block<Virus found>

• **Event** — Statistics.Counter.Increment<Default>("BlockedByAntiMalware", 1>

This means that rule tracing showed the request was blocked because the requested object had been found to be infected by a virus or other malware.

The blocking action was performed by a virus and malware filtering rule, which was processed in the response cycle when the object was received from a particular web server in response to the request.

The criteria of this rule included the Antimalware.Infected property. To find out what this property must be set to, the Anti-Malware engine on Web Gateway was called. It scanned the requested web object and detected an infection, so the property could be set to **true** and the rule criteria matched.

**Best practices - Find out why a web page displays no images**

Use rule tracing to find out why a requested web page appears on a client system, but with text only and without displaying any images.

Imagine a sample issue, where a user requests access to the CNN channel homepage from a browser on a client of Web Gateway. The page appears, but displays only text.

You can use rule tracing to see whether a CNN server that provides the images on the homepage might have been blocked and why this happened.
Task

1. On the user interface of Web Gateway, select Troubleshooting. If you are using several Web Gateway appliances in a Central Management configuration, make sure you are logged on to the appliance that the client in question is connected to.

2. On the troubleshooting tree, select Rule Tracing Central.

3. Create a trace.
   a. In the input field on the top left, type the IP address of the client system that had a request blocked, then click Go on the toggle button next to the input field.

   Requests for web access sent from the client are now traced and entries for trace files are displayed in the output field on the lower left.

   The Go on the toggle button turns into a cross to let you stop the process when no more tracing is needed.

   b. On the client system, refresh the browser or click or enter ccn.com again to reproduce the issue.

   Trace file entries appear in the output field on Web Gateway.

   Depending on the amount of data that is being transferred, it can take a while until the trace file entries appear.

   c. When you have reproduced the issue and the trace file entries have appeared, click the toggle button again to stop the tracing.

4. Review the trace file entries.

   For every request that has been traced, a time stamp and the requested URL are shown.

   At the beginning of an entry, a symbol for the most impacting action that was executed when processing the request is also shown. The most impacting of all actions is the Block action.

   When reviewing the trace file entries, you will see several entries with the blocking symbol and a URL beginning with cdn.turner.com/ccn. These are probably trace files for requests to access the CCN server that provides the images.

5. Select a trace file entry with cdn.turner.com/ccn.

   Information on this trace appears in the rules and details panes on the right.

6. Review the rules pane.

   The pane shows the rules that were processed for the request that was traced. The view stops at the last rule that applied before rule processing stopped. The rule is highlighted.

   This way you can see that Block URLs whose category is in Category Block List is the last rule that applied.

7. Review the details pane.

   On the two tabs of the details pane, more tracing information is shown.

   On the Top Properties tab, you will see, among other information, that the URL.Categories property had the value Business when the rule mentioned above was processed.

This completes your rule tracing activities for this issue. Images from the CNN server were not displayed because the URLs that were submitted for accessing this server have fallen into the Business category and this category is on a blocklist.
If you want to see the images displayed, you need to reconfigure the web security policy for your network and put, for example, `cdn.turner.com/ccn/*` on a URL whitelist.

**Restore removed rule traces to the rule tracing panes**

To restore rule traces that you have removed from the rule tracing panes, supply them from the rule traces directory of an appliance or import them in a source file. How removed rule traces can be restored to the rule tracing panes depends on whether they were created on the appliance you are currently logged on to or were imported to this appliance. Accordingly, you can supply them from the rule traces directory of the appliance or repeat the import of the source file.

**Tasks**

- **Restore removed rule traces from an appliance directory on page 489**
  
  When rule traces that you have removed from the rule tracing panes had been created on the current appliance, you can restore them from the directory of rule tracing files on that appliance.

- **Restore removed rule traces by importing a source file on page 489**
  
  When rule traces that you have removed from the rule tracing panes had previously been imported, you can restore them by importing the source file once again.

**Restore removed rule traces from an appliance directory**

When rule traces that you have removed from the rule tracing panes had been created on the current appliance, you can restore them from the directory of rule tracing files on that appliance.

**Task**

1. Select **Troubleshooting**.
2. On the troubleshooting tree, expand the appliance you want to restore rule traces on.
3. Select **Rule tracing files**.
   
   The directory of the rule tracing files appears on the right side of the troubleshooting page.
4. Under **Trace files**, select the rule tracing files you want to restore.
5. Click **Analyze**.

The rule traces are accessible again in the rule tracing panes.

**Restore removed rule traces by importing a source file**

When rule traces that you have removed from the rule tracing panes had previously been imported, you can restore them by importing the source file once again.

**Task**

1. Select **Troubleshooting**.
2. On the troubleshooting tree, select **Rule Tracing Central**.
3. Click **Traces** and then **Import**.
   
   The local file manager opens.
4. Browse to the location where you stored the zipped file that is the source for the rule traces you want to restore, select the file, and import it.

The rule traces are accessible again on the rule tracing panes.
Delete rule traces
To delete rule traces, access the directory of rule tracing files on an appliance and use the delete option that is provided.

**Task**
1. Select **Troubleshooting**.
2. On the troubleshooting tree, select the appliance you want to delete rule traces on, then click **Rule tracing files**. The directory of rule tracing files appears on the right side of the troubleshooting page.
3. Under **Trace files**, select the rule tracing files you want to delete and click **Delete**.
4. In the window that opens, confirm the deletion.

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.
   - 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 system and network tools

You can work with several system and 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 tool on and click **System Tools** or **Network Tools**.
The available system tools are:

- service restart
- AV threads

The available network tools are:

- ping and ping6
- nslookup
- traceroute and traceroute6
- ipneigh
- ntp

3. In the Command line parameters field, type the parameters for a command that can be executed by a particular tool.
   For example, type the name of a host you want to connect to using the ping network tool.

4. Click the button for the tool that you want to use.
   The corresponding command is executed and the resulting output displayed under Results.

   The following could, for example, be displayed:

   Ping: Unknown host testhost

   ![To export the results to a location within your file system, click Export and specify the location in the window that opens.]

---

**Restart a service of the operating system**

Using the restart tool, you can stop a service of the operating system that is currently running and restart it again. If a service is not running at the time when the tool is applied to it, the service is started.

![You cannot restart the main mwg service and the sysconfd service, which is a daemon for implementing manual configuration changes, using this system tool.]

**Task**

1. Select the Troubleshooting top-level menu.

2. On the appliances tree, select the appliance you want to start a service on and click System Tools.
3 In the **Command line parameters** field, type the service name and parameters as required.

4 Click **service restart**.

   The service is restarted and the executed service activities are displayed in the **Results** field.

   The following could, for example, be displayed after restarting the *iptables* service.

   ```text
   Flushing firewall rules: [OK]
   Unloading ip6tables modules: [OK]
   Applying ip6tables firewall rules: [OK]
   ```

   To export the results to a location within your file system, click **Export** and specify the location in the window that opens.

### Display running AV threads

You can display the threads that are currently running to perform anti-malware scanning activities. Seeing many threads lets you know that scanning a particular request or response is consuming a high amount of resources. The list of threads that is shown includes the threads that actually perform scanning activities, as well as the threads that deliver requests and responses to the scanning modules. Both kinds of threads are referred to as anti-malware working threads or simply as **AV threads**.

**Task**

1 Select the **Troubleshooting** top-level menu.

2 On the troubleshooting tree, select **System Tools**, then click **AV threads**.

   A list of the AV threads appears under **Results**.

   For each thread, an ID number is shown, the time when the thread was started, its current status, and other information.

   To export the thread list to a location within your file system, click **Export** and specify the location in the window that opens.

### Back up and restore an appliance configuration

You can store an appliance configuration in a backup file and use this file to restore the appliance configuration. When backing up the appliance configuration, you have the option of including the SSO credentials in the credential store in the backup file. Likewise, when restoring, you have the option of restoring the SSO credentials from the backup file to the credential store.

When restoring a backup, you have the option of restoring all configurations and accounts or only the data configured under the **Policy** top-level menu, which includes data on rules, lists, and settings.

Make sure the UTF-8 character format is used on your administration system for Web Gateway if you want to insert special characters, for example, German umlaut (ä, ö, ü), in the passwords that are required for encrypting and decrypting a backup.
**Task**

1. On the dashboard, select **Troubleshooting**.
2. On the appliances tree, select the appliance whose configuration you want to back up or restore, then click **Backup/Restore**.
3. To back up the appliance configuration:
   a. To include SSO credentials in the backup, select the **SSO Credentials** check box.
   b. Click **Back up to file**.
   c. In your local file manager, create or select the backup file.
4. To restore the appliance configuration:
   a. To include all configurations and accounts in the restore, select the **Configurations and Accounts** check box.
   b. To include SSO credentials in the restore, select the **SSO Credentials** check box.
   c. Click **Restore from file**.
   d. Confirm the message stating that you will be logged off during the restore.
   e. In your local file manager, select the backup file to use for restoring the appliance configuration.

**Reset the appliance password**

You can reset the appliance password, which is the root password that is required for working with the command line interface on a system console to access Web Gateway.

**Task**

1. On the user interface of Web Gateway, select **Troubleshooting**.
2. On the appliances tree, select the appliance you want to reset the root password on, then click **Reset appliance password**.
3. Type the new password in the input field that is provided, repeat it in the next field, then click **Change Password**.
   
The password must contain between 8 and 100 characters. It must at least include one upper-case and one lower-case alphabetical, as well as one non-alphabetical character.

   The password is reset.

   The reset is confirmed by a message under **Results**. If the password could not be reset or other issues occurred, this is also stated in this field.

To verify that the reset was actually performed, connect to the appliance from a system console using SSH. Use **root** as the user name and the password that you reset when you log on.

*You are not allowed to reset the root password in this way if you are running Web Gateway in FIPS mode.*
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)`
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.
Test a wildcard expression
Index

A

action
  add to rule 133
  rule element 127
  settings 165
administrator
  accounts 306
  external accounts 307
  roles 307
Advanced Threat Defense
  ATD - Offline Scanning with Immediate File Availability rule set 245
    configuring 240
    McAfee Advanced Threat Defense rule set 244
    monitoring 242
    monitoring with Content Security Reporter 242
    scanning criteria 235
    Use existing report 237
    use ongoing scanning run 238
    workflows 234
alerts 431
anti-malware filtering
  Advanced Threat Defense 232
  Anti-Malware module 170
  anti-malware queue 182
  Avira engine 170
  Gateway Anti-Malware engine 170
  Gateway Anti-Malware rule set 171
  Gateway Anti-Malware with TIE rule set 176
  host header missing 179
  lists 170
  media stream scanning 182
  process 169
  rules 170
  system settings 183
  threat protection 169
  TIE server integration 174
  using URL information 173
appliance
  administrator 306
  alerts 431
  back up configuration 493
  Central Management 94
  components 15
appliance (continued)
  configuration daemon 15
  configurator 15
  coordinator 15
  core 15
  dashboard 431
  error handling 448
  filtering cycles 121
  logging 434
  main functions 14
  operating system 15
  reset password on user interface 494
  restore configuration 493
  rules 127
  system architecture 15
  troubleshooting 483
application filtering
  blocking lists 202
  individual functions 202
  process 202
  rule set 206
  rules 202
  system lists 202
authentication
  IM Authentication rule set 283
  implement different method 262
  instant messaging 281
  LDAP digest authentication 264
  LDAP method 273
  McAfee Pledge 285
  one-time passwords 285
  system settings 262
Authority Information Access (AIA) entries 220
Avira engine 170

B

back up configuration 493
backup encryption 493
bandwidth control
  bandwidth throttling 344
bandwidth throttling
  basic bandwidth throttling 345
  methods 344
  non-proxy traffic 348
bandwidth throttling (continued)
using classes 347
best practices
adding a log file field 440
configuring authentication for deployment types 266
configuring Central Management node groups 101
configuring FTP over HTTP 63
configuring LDAP authentication 273
configuring the explicit proxy mode with WCCP 38
configuring the Proxy HA mode 33
configuring the Stream Detector 210
creating a log 441
fine-tuning a transparent bridge configuration 50
High Availability size limits 36
monitoring file system usage 466
sending access log data to syslog 469
sending TLS-secured syslog data 473
troubleshooting next-hop proxy issues 357
using URL properties for whitelisting 186
working with a McAfee-supplied subscribed list 152
working with progress indication methods 338
working with the error handler 450
working with the user-agent header 70
bonded interface 22
bonding interface 22
cloud connectors (continued)
generic IceToken, configuring 389
generic SAML2 368
generic SAML2, configuring 377
HTTP, configuring 372
predefined 366
SAML2, configuring 376
templates 365
templates, generic vs. individual 368
cloud storage encryption
Cloud Storage Encryption rule set 421
configure data encryption and decryption 420
configure settings 420
decrypt storage data 417
decrypt storage data manually 421
encrypt storage data 417
event log 358
encryption algorithms 417
high-level steps for data encryption and decryption 420
storage services 417
Common Catalog
enable use 157
list types 157
user account 158
configuration daemon 15
configurator subsystem 15
Content Security Reporter 242
Cookie authentication with SAML back end and fixed ACS URL rule set
about 383
Authenticate clients with authentication server 385
Authentication server request 386
Cookie authentication at authentication server 386
Cookie authentication at HTTP(S) proxy 384
Intercept SAML assertion if IdP uses a fixed ACS URL 384
Set cookie for authenticated clients 385
cordinator subsystem 15
core subsystem 15
criteria
add to rule 132
operand 127
operator 127
parameter 127
property 127
rule element 127
cycles
embedded objects 121
request 121
response 121
D
dashboard
access 432
alerts 431
charts and tables 431
Data Exchange Layer, See DXL
data loss prevention
  ICAP server 254
  logging 247
  process 247
  rule set 253
  rules 247
data trickling 336
DNS servers
  conditional forwarding 69
  use according to domains 69
DXL
  ePO 69
  messages 69
  scenarios 69
  security architecture 69
  TIE server 69
Dynamic Content Classifier
  configure use 193
  URL categories 193
E
  embedded objects cycle 121
Enterprise Security Manager 476
ePolicy Orchestrator 464
error handling
  using error IDs 448
  using incident information 448
ESM 476
ethernet bonding 22
  add to rule 134
  explicit proxy mode 32
  external lists
    module 145
    properties 145
    recommended use 145
    sources 145
F
filtering
  embedded objects cycle 121
  process flow 122
  request cycle 121
  response cycle 121
G
Gateway Anti-Malware engine 170
global whitelisting
  Global Whitelist rule set 212
  rule set 212
  rules 212
  whitelists 212
H
Hardware Security Module
  administrator responsibilities 226
  emulation) 226
  HSM Agent 226
  log module operations 226
  module card 226
  multiple appliances) 226
  nShield Solo (Thales 226
  OpenSSL) 226
  remote server (Gemalto) 226
  SafeNet Network (Gemalto) 226
  solutions 226
  store private keys 226
Helix proxy 91
  hybrid solution
    components 423
    configuring and enabling 428
    how it works 424
    management tasks 427
    restricted rules 427
  hybrid synchronization
    enabling a rule set 428
    verifying 429
I
ICAP communication
  secure ICAP 53
  use ICAP server for data loss prevention 254
IceToken authentication
  about 365
  compared to SAML 389
  inline lists 140
  instant messaging
    process 56
  isolated network updates 29
J
JavaScript Object Notation data (JSON) 159
L
launchpad
  customizing 391
  editing the Launchpad.html file 391
  providing custom logos 394
  style sheet, editing default 393
  style sheet, importing custom 394
LDAP
  authentication method 273
digest authentication 264
list
  access in rule 141
  access on Lists tab 141
  Common Catalog 157
list (continued)
create 142
custom lists 140
external lists 145
inline lists 140
subscribed lists 148
system lists 140
types 140
updatable system lists 140
logging
log files 434
modules 434
rules 434

P
policy configuration
configuring a rule element 123
enabling a rule set for cloud use 125
rule set views 115
web security policy 110
progress indication
best practices 338
data trickling 336
data trickling workflow 340
FTP upload timeout prevention workflow 341
progress page 336
progress page workflow 338
web browsers 338
property
add to rule 132
rule element 127
proxies
auto-configuration 89
conditional DNS forwarding 69
Data Exchange Layer settings 69
DXL 69
explicit proxy mode 32
FTP over HTTP 63
Helix 91
High Availability size limits 36
instant messaging 56
node communication protocols 68
Office 365 bypassing 74
outbound source IP addresses 61
Proxy HA mode 33
reverse HTTPS 77
SOCKS proxy 53
transparent bridge mode 46
transparent router mode 42
UDP protocol 55
user-agent header 70
using WCCP to redirect FTP traffic 66
WCCP 38
XMPP with SSL scanner disabled 60

Q
quota management
authorized override 320
blocking sessions 323
coaching 318
time quota 312

M
manual synchronization 429
McAfee Pledge 285
media stream scanning 182
media type filtering
blocking lists 198
configure key elements 199
Media Type Filtering rule set 198
rule set 198
rules 198
monitoring
dashboard 431
ePolicy Orchestrator 464
error handling 448
implementing TLS-secured usage of syslog data 473
logging 434
performance measurement 459
sending access log data to syslog 469
sending syslog data to ESM 476
SNMP agent 464

N
network interface bonding 22
next-hop proxies
failover mode 351
forward requests tp 350
modes 350
round-robin mode 350
rule set 360
SOCKS protocol 354
stickiness 352
troubleshooting 357
NIC bonding 22
node communication protocols 68

O
one-time passwords
configure for authenticating users 286
configure for authorized overriding 286
McAfee Pledge 285
one-time passwords (continued)
overview 285
online rule set library 114
operand 127
operating system 15
operator 127

Index
quota management (continued)
  volume quota 314

R
  request cycle 121
  response cycle 121
  restore configuration 493
  rule
    action 127
    create 131
    criteria 127
    elements 127
    event 127
    format on user interface 128
    operand 127
    operator 127
    process flow 122
    property 127
  representation in documentation text 129
  sets 112
  rule set
    create 135
    criteria 112
    cycles 112
    default system 113
    import 136
    library 114
    nested 112
    online library 114
    system 113
  rule sets
    not supported in the cloud 428
  rule tracing
    delete traces 490
    find reason for missing images 487
    overview 484
    restore traces 489

S
  SAML authentication, external Identity Providers
    about 377
    configuring 379
    Identity Provider URLs, adding to whitelists 381
    process 378
    requests, configuring settings 380
    responses, configuring settings 381
    responses, validating 382
    rule set 383
    SAML attribute mapping 381
    static ACS URLs, configuring 380
    static ACS URLs, support for 379
  SAML single sign-on
    about 373
    certificate management 375
  SAML single sign-on (continued)
    configuring external data sources 377
    Identity Provider (IdP) 373
    initiating 373
    Service Provider (SP) 373
  settings
    access 166
    access on Settings tab 166
    access in rule 167
    action 165
    create 167
    module 165
    system 165
    types 165
  Single Sign On rule set
    about 397
    exporting and importing 363
    Get Attributes in the Cloud 407
    Get Attributes on Premise 406
    Get Login Action 404
    HTTPS Handling 400
    Launchpad 401
    OTP Authentication 403
    Perform IceToken SSO 408
    Perform SAML SSO 407
    Perform SSO 409
    Process Common Tasks 408
    Select Services 398
  single sign-on
    cloud connectors 365, 366
    creating bookmarks 395
    credential model for HTTP applications 372
    data sources 365
    dynamic HTTP applications 371
    high-level configuration 362
    monitoring logons 395
    process in proxy and non-proxy modes 364
    resolving issues 416
    rule set reference 397
    rule set summary 396
    SSO Catalog 366
    supported authentication methods 365
    to .NET and Java web applications 389
    to HTTP applications and services 371
    to SAML applications and services 373
    using the launchpad 389
    viewing update status 370
  SNMP monitoring 464
  SOCKS protocol
    next-hop proxies 354
    SOCKS proxy 53
    SOCKS Proxy rule set 56
  SOCKS proxy
    configure settings 55
    source-based routing 25
SSL scanning
Authority Information Access (AIA) entries 220
client certificate list 218
Hardware Security Module 226
lists 214
modules 214
rules 214
SSL Scanner rule set 221
store private keys 226
tapping 220
whitelists 214

SSO Catalog
as a service 367
cloud connectors 366
technical note 366
viewing in the user interface 366, 367

SSO Connector lists
adding connectors 371
configuring cloud access 370
viewing in the user interface 367

SSO logging
enabling 410
overview 409
rule set reference 411
rule set, SSO access log 412
rule set, SSO stop logging 415
rule set, SSO trace log 414

streaming media filtering
best practices 210
rule 208

subscribed lists
create 149
retrieving content 148
updates 150

system architecture 15
system configuration
cache volume resizing 27
initial setup settings 20
system files 27
update handling 28

T
tabs
Administrator Accounts 306
Alerts 432
Charts and Tables 433
Threat Information Exchange, See TIE
TIE server integration
anti-malware filtering 174
DXL messages 69
event 174
Gateway Anti-Malware with TIE rule set 176
procedure 176
property 174
TIE server integration (continued)
sample rules 174
TLS (Transport Layer Security) protocol 473
transparent modes
bridge 46
router 42
troubleshooting
AV threads 493
back up configuration 493
backup encryption 493
connection tracing files 491
core files 490
display running AV threads 493
feedback files 490
methods 483
network tools 491
packet tracing files 491
reset appliance password 494
restart service 492
restore configuration 493
rule tracing 484
system tools 491

U
updates
automatic 28
manual 28
URL filtering
best practices - using URL properties for whitelisting 186
blocking lists 183
configure key elements 185
Dynamic Content Classifier 193
IFP proxy 195
module 183
own URL filter database 194
rule set 183
rules 183
URL Filter module 183
URL Filtering rule set 183
using URL properties for whitelisting 186
whitelists 183

user interface
complete rules view 118
key elements view 116
user message
edit text 327
modifying a block page 327
templates 325
text 325
types 325
variables 325
user-agent header 70
W

WCCP 38
web access on-premise and remote 423
web cache enabling 334
rule set 333
rules 333
Web Cache rule set 334
web filtering
Advanced Threat Defense 232
anti-malware filtering 169
application filtering 202
data loss prevention 247

web filtering (continued)
global whitelisting 212
media type filtering 198
SSL scanning 214
streaming media filtering 208
URL filtering 183
wildcard expressions
glob expressions 495
regular expressions 495
test 497

X
XMPP with SSL scanner disabled 60