A

System settings

System settings are used to configure the appliance system.

Contents

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 A-1 Global Anti-Malware Settings

Option	Definition
Number of threads for AV scanning	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.
Use at least as many AV threads as the number of CPU cores available	When selected, the number of AV threads use for scanning activities is at least the same as the number of available CPU cores.
Maximum number of jobs in the queue	Limits the number of requests or responses that can be moved to the anti-malware queue as jobs for the scanning modules.
Number of seconds a scanning job stays in the queue before being removed	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.

Central Management settings

The **Central Management** settings are used for configuring appliances that you administer as nodes in a common configuration.

Central Management Settings

Settings for basic communication parameters of a node in a Central Management configuration

Table A-2 Central Management Settings

Option	Definition
IP addresses and ports of this node for Central Management communication	Provides a list for entering the IP addresses and port numbers that a node uses to communicate with other nodes in a Central Management configuration.
Timeout for distributing messages to other nodes	Limits the time (in seconds) that is allowed for another node to respond to a message from the current node to the specified value. The time can range from 10 to 600 seconds. It is set on a slider scale.

The following table describes the elements of an entry in the IP addresses and ports list.

Table A-3 IP addresses and ports – List entry

Option	Definition
String	Specifies the IP address and port number for a node.
Comment	Provides a plain-text comment on an IP address and a port number.

Advanced Management Settings

Settings for advanced administration of a Central Management configuration

Table A-4 Advanced Management Settings

Option	Definition
Multiplier for timeout when distributing over multiple nodes	Sets a factor for increasing the time interval that has been configured under **Timeout for distributing messages to other nodes** in the *Central Management Settings* section. Increasing the time interval gives messages more time to proceed from one node to another, from there to the next node, and so on. The interval can be increased by a value between 1 and 2. The value is set on a slider scale.
Use and serve persistent connections	When selected, the nodes in a cluster use and serve persistent connections for their communication This option is selected by default on nodes that have been newly installed (clean install). It is not selected on existing nodes that have been updated. We recommend that you keep using persistent connections, which means that to ensure their use, you must also select the option on the updated nodes.
Node priority	Sets the priority that a node takes within a node group The highest priority is 1. If the configuration data on a node is no longer synchronized with that of other nodes, for example, because the node has been down for some time, the node receives the most recent configuration data from the node with the highest priority. If this is not your intention, make sure that all nodes have the same priority, which is also the recommended setting. The priority of a node can range from 1 to 100. It is set on a slider scale.
Allow a GUI server to attach to this node	When selected, a server providing an additional user interface for the appliance is allowed to connect to the node.
Allow to attach a GUI server from non-local host	When selected, a server with an additional user interface that is not running on the current node is allowed to connect to the node.
GUI control address	Specifies the IP address and port number the additional user interface uses for connecting to the current node.
GUI request address	Specifies the IP address and port number of this server used when sending requests to it.
Use unencrypted communication	When selected, messages sent from this node to other nodes in the configuration are not encrypted. However, authentication using certificates is still performed. This option is not selected by default. ℹ Make sure that all nodes in a Central Management configuration are configured in the same way with regard to this option Otherwise communication between the nodes will fail due to the differences in encryption handling.
Enable IP checking for other nodes	When selected, the IP address can be verified when messages are sent from this node to other nodes in the configuration. This function is intended to increase web security, but can lead to problems for some network setups, for example, NAT setups.

Table A-4 Advanced Management Settings *(continued)*

Option	Definition
Allowed time difference	Limits the time difference (in seconds) allowed for accepting configuration changes to the specified value. The number of seconds can range from 10 to 600. It is set on a slider scale.
Enable version checking for other nodes	When selected, the version of the appliance software is checked before configuration changes are distributed between nodes. Configuration changes are not distributed to a node if the version of the appliance software on this node does not match the version on the node that distributes the changes. • **Level of version check** – Sets a level of thoroughness when verifying the version of the appliance software. The level is set on a slider scale. It can take the following values: • 1 – Only major version number (7 in 7.3.0) must match. • 2 – Minor version number (3 in 7.3.0) must also match. • 3 – Feature version number (0 in 7.3.0) must also match. • 4 – Maintenance version number (if any, for example, 1 in 7.3.0.1.2) must also match. • 5 – Hotfix version number (if any, for example, 2 in 7.3.0.1.2) must also match. • 6 – Build number (for example, 14379) must also match.

This Node is a Member of the Following Groups

Settings for including a node in a group of nodes

Table A-5 This Node is a Member of the Following Groups

Option	Definition
Group runtime	Determines the group of a node, in which runtime data can be shared with all nodes in the group, for example, time quotas.
Group update	Determines the group of a node, in which updates can be shared with all nodes in the group
Group network	Determines the group of a node, in which the node can immediately connect to all other nodes in the group A node can be a member of more than one network group. In this case, the nodes of a group that a node is a member of can connect through this node to nodes of another group that this node is also a member of. All groups that a node is a member of are listed in the Group network list.

The following table describes the elements of a list entry in the group network list.

Table A-6 Group network – List entry

Option	Definition
String	Specifies the name of a network node group.
Comment	Provides a plain-text comment on a network node group.

Automatic Engine Updates

Settings for scheduling automatic updates of database information for modules used in the filtering process

Table A-7 Automatic Engine Updates

Option	Definition
Enable automatic updates	When selected, database information is automatically updated.
Allow to download updates from the internet	When selected, database updates are downloaded from the internet.
Allow to download updates from other nodes	When selected, database updates are downloaded from other nodes in a Central Management configuration.
Update interval	Limits the time (in minutes) that elapses before database information is again updated to the specified value. The time is set on a slider scale. Allowed values range from 15 to 360.
CRL update interval	Limits the time (in hours) that elapses before certificate revocation lists used in filtering SSL-secured web traffic are updated to the specified value. This update uses a method that differs from those of other updates and must therefore be configured separately. The time is set on a slider scale Allowed values range from 3 to 168.
Enable update proxies	When selected, proxies are used for performing updates. The proxies are configured in the **Update proxies (fail over)** list. These proxies are also used when the MLOS operating system of a Web Gateway appliance is updated.
Update proxies (fail over)	Provides a list for entering the proxies that are used for performing updates. The proxies are used in failover mode. The first proxy on the list is tried first and only if the configured timeout has elapsed is the next proxy tried.

The following table describes the elements of an entry in the **Update proxies** list.

Table A-8 Update proxies – List entry

Option	Definition
Host	Specifies the host name or IP address of a proxy for performing updates.
Port	Specifies the port on a proxy that listens for update requests.
User	Specifies the name of a user who is authorized to access a proxy for performing updates.
Password	Sets a password for this user.
Comment	Provides a plain-text comment on a proxy.

Advanced Update Settings

Settings for advanced update functions

Table A-9 Advanced Update Settings

Option	Definition
Allow to upload updates to other nodes	When selected, updated database information can be uploaded from the appliance (as a a node in a Central Management configuration) to other nodes.
The first time an update starts, it should wait an appropriate time before starting	Limits the time (in seconds) that elapses before an update is started to the specified value. Allowed values range from 5 to 1200.

Table A-9 Advanced Update Settings *(continued)*

Option	Definition
The first time an automatic update starts, it uses the startup interval to update	Limits the time (in seconds) that elapses between attempts to start an automatic update for the first time to the specified value. During an update, the coordinator subsystem, which stores updated information on the appliance, tries to connect to the appliance core, where the modules reside that use this information. A low value for this interval can therefore speed up updates because it reduces the time the coordinator might have to wait until the core is ready to receive data. Allowed values range from 5 to 600.
Try to update with start interval	Limits the number of attempts (1 to 9) the appliance makes when trying to start an update to the specified value.
Use alternative URL	Specified the URL of an update server that is used instead of the default server.
Verify SSL tunnel	When selected, a certificate sent to a node by an update server in SSL-secured communication is verified.
Enter a special custom parameter sequence for an update server	Updates of URL filtering information are taken from the URL filter database server that is specified by the URL entered here.
No updates should be made in defined time window	Provides a list for entering daily time slots during which no updates of database information should be made.

The following table describes the elements of an entry in the time slot list.

Table A-10 Time slot – List entry

Option	Definition
Start of time slot (hour)	Sets the hour when a daily time slot begins.
Start of time slot (minute)	Sets the minute in an hour when a daily time slot begins.
Start of time slot (second)	Sets the second in a minute when a daily time slot begins.
End of time slot (hour)	Sets the hour when a daily time slot ends.
End of time slot (minute)	Sets the minute in an hour when a daily time slot ends.
End of time slot (second)	Sets the second in a minute when a daily time slot ends
Comment	Provides a plain-text comment on a time slot.

Advanced Subscribed Lists Settings

Settings for advanced subscribed lists functions

Table A-11 Advanced Subscribed Lists Settings

Option	Definition
Allow to download customer subscribed lists	When selected, customer subscribed lists can be downloaded from the current appliance. If the appliance is a node in a Central Management configuration and this option is also selected on other nodes, one of the nodes will download the lists. If you want a particular node to download the lists, you need to make sure the option is deselected on every other node. When a node is restarted and one or more subscribed lists are configured on this node, list content is downloaded to ensure a valid configuration. ℹ The download is performed regardless of whether this download option is selected or not. When a node is added to a configuration with other nodes that have subscribed lists configured, list content is downloaded for these lists onto the new node. To reduce internal traffic, the download is performed without prior communication with other nodes. ℹ The download is performed regardless of whether this download option is selected or not.

Manual Engine Updates

Setting for performing manual updates of database information for modules used in the filtering process

Table A-12 Manual Engine Updates

Option	Definition
Manual Engine Update	Updates database information for modules used in the filtering process immediately. Database information is only updated for the modules on the appliance you are currently working on.

Handle Stored Configuration Files

Settings for storing configuration file folders on disk

Table A-13 Handle Stored Configuration Files

Option	Definition
Keep saved configuration folders for a minimal time	Limits the time (in days) that configuration file folders are at least stored on disk to the specified value. The number of days can range from 1 to 100.
Keep minimal number of configuration folders	Limits the number of configuration file folders that are at least stored on disk at any time to the specified value. The number can range from 1 to 100.
Keep minimal number of packed folders	Limits the number of packed configuration file folders that are at least stored on disk at any time to the specified value. Configuration folders are packed when the minimal time configured for storing them on disk has elapsed and the minimal number of folders stored on disk at any time would be exceeded if they were stored unpacked any longer. The number of folders can range from 1 to 100.

Advanced Scheduled Jobs

Settings for scheduled jobs

Table A-14 Advanced Scheduled Jobs

Option	Definition
Job list	Provides a list of scheduled jobs.

The following table describes the elements of a list entry.

Table A-15 Job list – List entry

Option	Definition
Start job	Specifies the time setting for starting a scheduled job, for example, *hourly*, *daily*, *once*.
Start job immediately if it was not started at its original schedule	Lets a scheduled job start immediately if this has not happened according to the originally configured schedule.
Job	Specifies the type of job, for example, *Backup Configuration*.
Unique job ID	Identifies a scheduled job.
When this job has finished run job with ID	Provides the ID of a job that is run immediately after this job.
Comment	Provides a plain-text comment on a scheduled job.

Add Scheduled Job window

Provides settings for adding a scheduled job

- **Time Settings** — Settings for the time when a scheduled job is started
- **Job Settings** — Settings for the type and ID of a scheduled job
- **Parameter Settings** — Settings for additional parameters of a scheduled job

  These settings differ for each job type as follows:

  - (Backup configuration settings) — Settings for a scheduled job that creates a backup of an appliance configuration
  - (Restore backup settings) — Settings for a scheduled job that restores a backup of an appliance configuration
  - (Upload file settings) — Settings for a scheduled job that uploads a file to an external server using the HTTP or HTTPS protocol
  - (Download file settings) — Settings for a scheduled job that downloads a file to the appliance using the HTTP or HTTPS protocol

  For a scheduled job that performs a yum update, there are no additional parameter settings.

Table A-16 Time Settings

Option	Definition
Start job	Lets you select a time setting. • **Hourly** — Starts a scheduled job every hour • **Daily** — Starts a scheduled job once on a day • **Weekly** — Starts a scheduled job once in a week • **Monthly** — Starts a scheduled job once in a month • **Once** — Starts a scheduled job only once • **Activated by other job** — Starts a scheduled job after another job has been completed
(Time parameter settings)	Settings specifying the parameters for a time setting, for example, the minute in an hour when a job scheduled for hourly execution should be started Which time parameter settings are shown depends on the selected time setting. For example, if you have selected *Hourly*, you can configure the minute in an hour, but not the day in a month. • **Minute** — Sets a minute in an hour • **Hour** — Sets an hour on a day • **Day of month** — Sets a day in a month • **Enter day of week** — Provides a list for setting a day in a week • **Month** — Sets a month in a year (specified by a number from 1 to 12) • **Year** — Sets a year (four digits)
Start job immediately if it was not started at its original schedule	When selected, a scheduled job is started immediately if this has not happened according to the originally configured schedule. This can be the case, for example, when an appliance is temporarily shut down due to overload and a job was scheduled to run during this downtime. The job is then executed as soon as the appliance is up again.

Table A-17 Job Settings

Option	Definition
Job	Lets you select the type of a scheduled job. • **Backup configuration** — Creates a backup of an appliance configuration • **Restore backup** — Restores a backup of an appliance configuration • **Upload file** — Uploads a file to an external server using the HTTP or HTTPS protocol • **Download file** — Downloads a file onto the appliance using the HTTP or HTTPS protocol • **Yum update** — Performs a yum update on an appliance configuration ℹ This scheduled job type is not available when an appliance runs in a FIPS-compliant mode
Unique job ID	Identifies a scheduled job. The characters specified in this string are case-sensitive
Job description	Provides an optional description of a scheduled job in plain-text format.

Table A-17 Job Settings *(continued)*

Option	Definition
When this job has finished run job with ID	Provides the ID of a scheduled job that is to run immediately after the job configured here has finished. For this job, you must have configured the **Activated by other job** time setting.
Execute job on remote node	Provides a list for selecting other nodes of the configuration to execute a scheduled job. The list displays the host names for the other nodes. The scheduled job that you configure on this appliance is executed with its time and parameter settings on the selected node or nodes. A message is sent to the other node or nodes to inform them about the scheduled job.

Table A-18 Parameter Settings – Backup configuration

Option	Definition
Use most recent configuration	When selected, the scheduled job creates a backup from the most recent appliance configuration Format: |*<path name>/<file name with extension>*
Backup configuration path	Specifies the name of the path to the folder where the configuration is stored that should be used for the backup. Format: */opt/mwg/storage/default/configfolder* This setting is only available when **Use most recent configuration** is deselected.
Save configuration to path	Specifies the path and file name for a backup configuration. Format: */<path name>/<file name with file name extension>* You must set user rights for the folder you want to store the backup configuration in, making the appliance the owner who is allowed to write data into the folder. On the command line provided, for example, by a serial console, run the appropriate commands to create a folder or change the rights for an existing folder.

Table A-19 Parameter Settings – Restore backup

Option	Definition
Restore backup from file	Specifies the path and file name for the file that should be used to restore a backup. Format: |*<path name>/<file name with extension>*
Only restore policy	When selected, a scheduled job backs up only settings related to the web security policy that was implemented on an appliance. Other settings, for example, settings needed for connecting an appliance to a network are not restored.
Lock storage during restore	When selected, no other files can be stored on the appliance until the scheduled job has completely restored the backup configuration.
Password	Sets a password that is submitted for basic authentication.
Set	Opens the **New Password** window for setting a password. When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password. This setting is only available when **Enable basic authentication** is selected.

Table A-20 Parameter Settings – Upload file

Option	Definition
File to upload	Specifies the path and file name for a file that should be uploaded. Format: |<*path name*>/<*file name with extension*>
Destination to upload file to	Specifies the name of the path to the server that a file should be uploaded to under the HTTP or HTTPS protocol and the file name for storing the file on the server. Format: *http*|*https: //*<*URL*>/<*file name with extension*>
Enable basic authentication	When selected, basic authentication is required for uploading a file.
User name	Specifies a user name that is submitted for basic authentication. This setting is only available when **Enable basic authentication** is selected.
Password	Sets a password that is submitted for basic authentication.
Set	Opens the **New Password** window for setting a password. When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password. This setting is only available when **Enable basic authentication** is selected.

Table A-21 Parameter Settings – Download file

Option	Definition
URL to download	Specifies a URL for the location of a file that should be downloaded under the HTTP or HTTPS protocol and the name of the file. Format: *http*|*https: //*<*URL*>/<*file name with extension*>
Save downloaded file to	Specifies a path to the location where a downloaded file should be stored and the file name for storing the file. Format: |<*path name*>/<*file name with extension*>
Enable basic authentication	When selected, basic authentication is required for downloading a file
User name	Specifies a user name submitted for basic authentication. This setting is only available when **Enable basic authentication** is selected.
Password	Sets a password that is submitted for basic authentication.
Set	Opens the **New Password** window for setting a password. When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password. This setting is only available when **Enable basic authentication** is also selected.

Special updates (for an OEM use case only)

Settings for updating TrustedSource data used in the URL filtering process on a Central Management cluster of appliances

You can configure these settings to integrate an externally created, customized URL filtering list file in this process.

> You need an OEM agreement with McAfee to obtain a license for the tools that are required to create the external URL filtering list file.

Operating a Central Management cluster in the usual way does not require this list file.

Table A-22 Special updates

Option	Definition
Enable separate download of TrustedSource Database	When selected, the TrustedSource Database can be downloaded separately according to what you configure for this process.
Manual Update	Triggers a manual update of the database.
Download URL	Specifies a URL for downloading the database.
User	Specifies a user name that is submitted for the download.
Password	Sets a password that is submitted for the download.
Set	Opens the **New Password** window for setting a password. When a password has been set, the **Set** button is replaced by a **Change** button, which opens the **New Password** window for changing a password.
Enable download by interval	When selected, the TrustedSource Database can be downloaded in intervals according to what you configure for this process.
Update interval	Sets the time (in minutes) that elapses before the database is downloaded again. The time is set on a slider scale. Time range: 15-1440 minutes
Enable update proxies	When selected, proxies are used for downloading the TrustedSource Database according what you configure for this process.
Update proxies	Lists the proxies that have been set up to enable a download of the database.

The following table describes the elements of an entry in the **Update proxies** list.

Table A-23 Update proxies – List entry

Option	Definition
Host	Specifies a host name for an update proxy.
Port	Specifies a port on the host for an update proxy.
User	Specifies a user name that is submitted for running an update proxy.
Password	Sets a password that is submitted for running an update proxy.
Comment	Provides a plain-text comment on an update proxy

Coaching system settings

Coaching system settings are general settings for time intervals related to quota management.

If an appliance is a node in a Central Management configuration, you can configure time intervals for data synchronization with other nodes.

These settings are configured on the **Appliances** tab of the **Configuration** top-level menu.

They can also appear under the name of *Quota* (instead of Coaching), They apply in both cases to all options that are provided for quota management: Authorized override, blocking sessions, coaching, time quota, and volume quota.

Quota Intervals for Synchronisation and Saving in Minutes

Settings for time intervals related to quota management

Table A-24 Quota Intervals for Synchronisation and Saving in Minutes

Option	Definition
Enable synchronization of quota data	When selected, quota data is synchronized according to what you configure for this process
Save interval	Sets the time (in minutes) that elapses before current quota values are saved again on an appliance. Quota values to be saved are, for example, the byte volumes that have been consumed by users.
Interval for sending updated quota data	Sets the time (in minutes) that elapses before current quota values are distributed again from an appliance to all nodes in a Central Management configuration. The distributed data includes the changes in quota values that have occurred since the last time that data were distributed from the appliance.
Interval for base synchronisation	Sets the time (in minutes) that elapses before quota values are synchronized again on all nodes in a Central Management configuration. The synchronization takes a snapshot of the current quota values on all appliances. The values that are most recent with regard to individual users are distributed to all appliances. The values are also distributed to nodes that were temporarily inactive and did not receive updates sent during that time. They are, furthermore, distributed to nodes that have been newly added to the configuration, so they did not receive any previous updates.
Cleanup database after	Sets the time (in days) that elapses before data is deleted in the quota database. Before data is deleted, a check is performed to see whether the data is obsolete. Data is obsolete if the time interval that has been configured for a quota management function has elapsed. For example, if a particular amount of bytes has been configured as volume quota for a user to be consumed during a month, the amount that the user actually consumed during a month becomes obsolete when a new month begins. The cleanup then deletes this data if the time configured under the **Cleanup database after** option has also elapsed. Stored data becomes obsolete after a month for time quotas. For other quota management functions, other time intervals are relevant. For example, for coaching and authorized overriding, the cleanup cannot be performed before the allowed session time has elapsed.

Date and Time settings

The **Date and Time** settings are used for configuring the time servers that synchronize date and time of the appliance system. They also allow you to set the system time manually.

Date and Time

Settings for date and time of the appliance system

Table A-25 Date and Time

Option	Definition
Enable time synchronization with NTP servers	When selected, the appliance uses time servers under the NTP (Network Time Protocol) for time synchronization. The system time of the appliance is then synchronized with the time on the NTP servers. This will fail, however, if the delta between both times is too big. **Best practice**: Restart the appliance after configuring time synchronization with NTP servers. When the appliance restarts, it sets system time to the time on the NTP servers.
NTP server list	Provides a list for entering the servers that are used for time synchronization under the NTP protocol. The list elements are as follows: • **String** — Specifies the name of an NTP server. • **Comment** — Provides a plain-text comment on an NTP server.
Select time zone	Provides a list for selecting a time zone. Time synchronization performed by the NTP servers or manually set time refer to the time zone that you select here

Set System Time Manually

Settings for configuring time and date on the appliance system manually

Table A-26 Set System Time Manually

Option	Definition
Current date and time	Provides items for setting date and time of the appliance system. • **Date** — Enables you to enter a date by typing it in the field or using a calendar. • Calendar icon — Opens a calendar for selecting a date. After selecting a date on the calendar and clicking **OK**, the date appears in the date field. • **Time** — Lets you specify a time by typing it. The system time of an appliance is then synchronized with the time on the NTP servers. This will fail, however, if the delta between both times is too big. **Best practice**: Restart the appliance after configuring time synchronization with NTP servers. When the appliance restarts, it sets system time to the time on the NTP servers.
Set now	Sets the date and time you have entered into the corresponding fields.

DNS settings

The DNS settings are usedr for configuring the domain name servers an appliance connects to for retrieving IP addresses that match the host names submitted in user requests.

Domain Name Service Settings

Settings for the IP addresses of different domain name servers

Table A-27 Domain Name Service Settings

Option	Definition
Primary domain name server	Specifies the IP address of the first server.
Secondary domain name server	Specifies the IP address of the second server.
Tertiary domain name server	Specifies the IP address of the third server.

ePolicy Orchestrator settings

The **ePolicy Orchestrator** settings are used for configuring the transfer of monitoring and other data from a Web Gateway appliance to a McAfee ePO server.

ePolicy Orchestrator Settings

Settings for transferring monitoring data to a McAfee ePO server

Table A-28 ePolicy Orchestrator Settings

Option	Definition
ePO user account	Specifies a user name for the account that allows the retrieval of monitoring data from an appliance.
Password	Sets a password for a user. Clicking **Change** opens a window for setting a new password.
Enable data collection for ePO	When selected, monitoring data for the McAfee ePO server is collected on an appliance.
Data collection interval in minutes	Limits the time (in minutes) that elapse between data collections. The time is set on a slider scale, ranging from 10 minutes to 6 hours.

ePO DXL Settings

Settings for configuring the credentials submitted by Web Gateway when connecting to a McAfee ePO server to enable DXL messaging

Table A-29 ePO DXL Settings

Option	Definition
ePO host name	Specifies the host name that Web Gateway uses when connecting to a McAfee ePO server.
ePO user account	Specifies a name for the user account that Web Gateway submits when connecting to a McAfee ePO server.
ePO user password	Sets the password that Web Gateway submits when connecting to a McAfee ePO server. Clicking **Set** opens a window for setting a new password.
ePO server port	Specifies the port on the McAfee ePO server that listens to requests sent from Web Gateway. Default port: 8443

Table A-29 ePO DXL Settings *(continued)*

Option	Definition
Agent handler port	Specifies the agent handler port that is used for communication between the McAfee ePO server and Web Gateway. Default port: 443
Rejoining ePO for DXL communication	When clicked, rejoins communication with the McAfee ePO server to complete the setup. A message informs you of the result.

External Lists system settings

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

Global Configuration

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

Table A-30 Global Configuration

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

File Data Source Configuration

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

Table A-31 File Data Source Configuration

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

Web Data Source Configuration

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

Table A-32 Web Data Source Configuration

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

File Server settings

The **File Server** settings are used for configuring dedicated file server ports on a Web Gateway appliance to enable, for example, file downloads by clients.

HTTP Connector Port

Settings for dedicated file server ports on an appliance

Table A-33 HTTP Connector Port

Option	Definition
Enable dedicated file server port over HTTP	When selected, the dedicated HTTP file server ports that are configured on an appliance are enabled.
HTTP connector	Specifies a dedicated HTTP port for connecting to the file server. You can enter more than one port here, separating entries by commas. Ports can range from 1024 to 65335. To set up ports within the range from 1 to 1023, you can create a port forwarding rule. Together with a port, you can enter an IP address. This means connecting to a file server on an appliance over this port requires that you specify both the port and this IP address. For example, there are two interfaces for connecting on an appliance with these IP addresses: eth0: 192.168.0.10, eth1: 10.149.110.10 You enter this under **HTTP connector**: `4711, 192.168.0.10:4722` Then connecting to a file server on the appliance over port 4711 is allowed using both IP addresses, whereas connecting over port 4722 requires that IP address 192.168.0.10 is used. Restricting connections in this way might be useful, for example, if you want to set up an intranet.
Enable dedicated file server port over HTTPS	When selected, the dedicated HTTPS file server ports that are configured on an appliance are enabled.

Table A-33 HTTP Connector Port *(continued)*

Option	Definition
HTTPS connector	Specifies a dedicated HTTPS port for connecting to the file server. You can enter more than one port here, separating entries by commas. Ports can range from 1024 to 65335. To set up ports within the range from 1 to 1023, you can create a port forwarding rule. Entering a port together with an IP address can be done in the same way as under **HTTP connector** and has the same meaning. Using the following options, you can specify a protocol and a list of valid ciphers for the HTTPS communication. • **SSL protocol version** — Specifies the version of the SSL protocol that is used for communication with the file server. You can select one of these versions or any combination of them. • **TLS 1.2** • **TLS 1.1** • **TLS 1.0** • **Server cipher list** — Specifies a string of Open SSL symbols used for encrypting communication with the file server.
Enable protection against cross-site scripting	When selected, the communication with the file server is protected against cross-site scripting. When a cross-site scripting attack is launched, malicious JavaScript code is inserted into messages that are sent during the communication. Adding the following header to messages prevents the execution of this attack: Header name: X-XSS-Protection Header value: 1
Enable protection against clickjacking	When selected, the communication with the file server is protected against clickjacking. When a clickjacking attack is launched, messages that are sent during the communication are embedded in iFrames, which can be used to steal data. Adding the following header to messages prevents the execution of this attack: Header name: X-Frame-Options Header value: DENY

Hybrid settings

When configured, the hybrid settings allow Web Gateway to connect to and communicate with McAfee WGCS.

Hybrid synchronization

The Web Gateway policy is synchronized with McAfee WGCS at the interval you specify in the hybrid settings. You can also perform synchronization manually. Manual synchronization doesn't affect the synchronization interval or schedule which continues as before.

Configuring the hybrid settings

The hybrid settings allow you to configure synchronization without a proxy server.

Table A-34 Web Hybrid Configuration

Option	Definition
Synchronize policy to Cloud	When selected, allows you to configure the **Web Hybrid** settings and enables the hybrid solution.
Appliance for Synchronization	From the drop-down list, select the Web Gateway appliance whose policy you want synchronized with McAfee WGCS. If you are running multiple appliances in a Central Management configuration, this setting ensures that the McAfee WGCS policy is always synchronized with the same appliance.
Cloud address	Specifies the address that Web Gateway uses to communicate with McAfee WGCS. **Value:** `https://msg.mcafeesaas.com:443`
Cloud administrator account name	Specifies your McAfee ePO Cloud user name.
Cloud administrator account password	Specifies your McAfee ePO Cloud password. To change the password, click **Set**, then enter the new password and click **OK**.
Customer ID	Specifies your McAfee WGCS customer ID.
Local policy changes will be uploaded within the same interval as defined below	Specifies the synchronization interval. **Default:** 15 minutes **Range:** 10–60 minutes

Configuring the advanced hybrid settings

The advanced hybrid settings allow you to add a proxy server to the configuration.

Table A-35 Advanced Synchronization Settings

Option	Definition
Verify server certificate on SSL connections	When selected, Web Gateway verifies the proxy server certificate for SSL connections.
Use a proxy for synchronization	When selected, allows you to configure the proxy server settings. When the settings are configured, the Web Gateway policy is pushed to McAfee WGCS through the proxy server.
Proxy host	Specifies the IP address or host name of the server which is used as a proxy.
Proxy port	Specifies the port number on the proxy server that listens for Web Gateway requests to transfer synchronization data. **Default:** 8080
Proxy user	Specifies the user name that Web Gateway sends to the proxy server when transferring synchronization data.
Proxy password	Specifies the password that Web Gateway sends to the proxy server when transferring synchronization data. To change the password, click **Set**, then enter the new password and click **OK**.

Kerberos Administration settings

The Kerberos Administration settings are specific settings for the Kerberos authentication method.

Kerberos Administration

Settings for the Kerberos authentication method

Table A-36 Kerberos Administration

Option	Definition
Key tab file	Specifies the file that contains the master key required to access the Kerberos server. You can type a file name or use the **Browse** button to browse to the file and enter its name in the field. When a ticket is issued for authentication according to the Kerberos method, the master key is read on the appliance and used to verify the ticket. If you are running a load balancer that directs web requests to the appliance, tickets are issued for the load balancer and verified on the appliance. It is then not checked whether a request is directed to the appliance.
Kerberos realm	Specifies an administrative domain configured for authentication purposes. Within the boundaries of this domain the Kerberos server has the authority to authenticate a user who submits a request from a host or using a service. The realm name is case sensitive, however. normally only uppercase letters are used, and it is good practice to make the realm name the same as that of the relevant DNS domain.
Maximal time difference between appliance and client	Limits the time (in seconds) that the system clocks on the appliance and its clients are allowed to differ to the specified value. Configuring Kerberos as the authentication method can lead to problems when particular browsers are used for sending requests: • When the Microsoft Internet Explorer is used in a version lower than 7.0, Kerberos authentication might not be possible at all. • When this explorer runs on Windows XP, Kerberos authentication might not work as expected. • When Mozilla Firefox is used, Kerberos authentication must be configured in the browser settings to enable this authentication method.
Enable replay cache	When selected, a ticket that is issued for authentication cannot be used more than once. ℹ Selecting this option reduces authentication performance

License settings

The **License** settings are used for importing a license to an appliance. Information about the license is shown together with these settings, and options for reviewing the agreements on license and data usage.

License Administration

Settings for importing a license

Table A-37 License Administration

Option	Definition
Import license	Provides the options that are required for importing a license.
I have read and accept the end user license agreement	Provides a link to the End User License Agreement and a checkbox to select after reading the document. To import a license, the checkbox must be selected, otherwise the import options remains grayed out.

Table A-37 License Administration *(continued)*

Option	Definition
License file	Shows the name and path of the license file that has been selected after browsing the local file system. When the name and path appear in this field, more license information is shown under **License information**. The license is activated by clicking **Save Changes**.
Browse	Opens the local file system to let you browse for a license file.

License Information

Information about an imported license and an option for reviewing the Data Usage Statement

Table A-38 License Information

Option	Definition
Status	Shows the name of a license file.
Creation	Shows the date when a license file was created.
Expiration	Shows the date when a license file expires.
License ID	Shows the ID of a license.
Customer	Shows the name of the license owner.
Customer ID	Shows the ID of the license owner.
Seats	Shows the number of workplaces in the license owner's organization that the license is valid for,
Evaluation	Shows whether the license has been evaluated.
Features	Lists the features of Web Gateway that are covered by the license.
I have read and understood the data usage statement	Provides a link to the Data Usage Statement.

Mobile Cloud Security settings

The **Mobile Cloud Security** settings are used to provide certificates and user-related information for the McAfee Mobile Cloud Security (MMCS) solution.

CA Certificates to Identify Mobile Devices

Settings for providing CA certificates

Option	Definition
CA certificates	Provides a list with entries for every CA certificate that has been added on Web Gateway. Each CA certificate is issued for use with a particular mobile device. To make these certificates available for cloud use, cloud synchronization must be enabled. You can enable this synchronization as an option of the **Web Hybrid** settings.

Table A-39 CA certificates - List entry

Option	Definition
Certificate	Specifies the name of a CA certificate file.
User	Specifies the name of a mobile device user that the CA certificate has been issued for.
User group	Specifies the name of the user group that the user belongs to. Specifying user group information is optional.
Comment	Provides a comment on a CA certificate in plain text.

Device Certificates Test

Settings for performing a certificate test

Option	Definition
Test device certificates	Clicking this button opens a window where you can perform a test for a CA certificate.

Mobile Device Management Solution

Settings for managing mobile devices

Option	Definition
VPN gateway address information	Provides a VPN Gateway address. You must specify this address when configuring a mobile device using a particular management solution.

Network Interfaces settings

The **Network Interfaces** settings are used for configuring the network interfaces of an appliance.

Configuring network interfaces

When configuring network interfaces on Web Gateway, we recommend setting up at least two and dedicating them to different purposes to ensure more resilience and higher throughput in every field of activities.

As a minimum, we recommend that you configure the following:

- Proxy network interface for proxy traffic
- Management network interface for all management-related traffic, such as user-interface traffic, cluster-communication traffic, or logging traffic

For more complex networks, we recommend configuring more network interfaces for different purposes. You might, for example, configure one interface for each of these fields of activities:

- Inbound proxy traffic
- Outbound proxy traffic
- Access to the Web Gateway user interface

  In a cluster of Web Gateway appliances, you might also run one appliance as a dedicated "UI appliance" to prevent increased user-interface access from impacting proxy traffic filtering.

- Cluster communication
- Pushing and pulling log files

To improve performance even further, you can also configure network bonding, which means that two or more network interfaces are combined to run as a single interface.

Network Interface Settings

Settings for network interfaces

Table A-40 Network Interface Settings

Option	Definition
Host name / Fully qualified domain name	Specifies the host name of an appliance. The name must be specified as fully qualified domain name.
Default gateway (IPv4)	Specifies the default gateway for web traffic under IPv4.
Default gateway (IPv6)	Specifies the default gateway for web traffic under IPv6.
Enable these network interfaces	Provides a list of network interfaces that are available for being enabled or disabled. The *eth0* network interface is by default included in the list and enabled.
IPv4	Provides options for configuring network interfaces under IPv4. The options are provided on a separate tab.
IPv6	Provides options for configuring network interfaces under IPv6. The options are provided on a separate tab.
Advanced	Provides options for configuring additional media. The options are provided on a separate tab.
Add VLAN	Opens a window for adding a network interface for VLAN traffic. You can use this option to run VLANs under IPv4 or IPv6. To add a network interface, you specify a number as its ID and click **OK**. The interface name is composed of two parts, separated by a dot. The first part is the name and number of the interface that is enabled in the list of available network interfaces. The second part is the number that you specify. For example, if the *eth0* interface is enabled and you specify 1, a network interface for VLAN traffic is added as *eth0.1*. It is initially not enabled. The range of numbers for VLAN network interfaces is 1–4094. After adding one or more network interfaces for VLAN traffic, you must also add their IDs to the parameters of the port redirects for the network mode that you are using. The window for adding or editing port redirects provides the **Optional 802.1Q VLANs** field for entering VLAN IDs. Separate multiple entries by commas.
Delete	Deletes a selected network interface for VLAN traffic.

The following tables describe the options on the **IPv4**, **IPv6**, and **Advanced** tabs.

IPv4

Tab for configuring network interfaces under IPv4

Table A-41 IPv4

Option	Definition
IP settings	Lets you select a method to configure an IP address for a network interface. • **Obtain automatically (DHCP)** — The IP address is automatically obtained, using the Dynamic Network Host Protocol (DHCP). • **Configure manually** — The IP address is configured manually. • **Disable IPv4** — IPv4 is not used for this interface.
IP address	Specifies the IP address of a network interface (manually configured).
Subnet mask	Specifies the subnet mask of a network interface (manually configured).
Default route	Specifies the default route for web traffic using the network interface (manually configured).
IP aliases	Provides a list of aliases for the IP address. • **Add alias** — Opens the Input window for adding an alias. To enable usage of an alias, you must restart Web Gateway. After entering an alias here, an alert reminds you of the restart. You can perform the restart by running the following command from the command line of a system console: `service mwg restart` • **Delete** — Deletes a selected alias.

IPv6

Tab for configuring network interfaces under IPv6

Table A-42 IPv6

Option	Definition
IP settings	Lets you select a method to configure an IP address for a network interface. • **Obtain automatically (DHCP)** — The IP address is automatically obtained, using the Dynamic Network Host Protocol (DHCP). • **Solicit from router** — The IP address is obtained from a router. • **Configure manually** — The IP address is configured manually. • **Disable IPv6** — IPv6 is not used for this interface.
IP address	Specifies the IP address of a network interface (manually configured).

Table A-42 IPv6 *(continued)*

Option	Definition
Default route	Specifies a default route for web traffic using the network interface (manually configured).
IP aliases	Provides a list of aliases for the IP address. • **Add alias** — Opens a window for adding an alias. To enable usage of an alias, you must restart Web Gateway. After entering an alias here, an alert reminds you of the restart. You can perform the restart by running the following command from the command line of a system console: `service mwg restart` • **Delete** — Deletes a selected alias.

Advanced

Tab for configuring advanced network interface functions.

> The tab provides different options when the currently selected network interface is a bonding interface. These options are described in a second table.

Table A-43 Advanced

Option	Definition
Media	Lets you select additional media for use with a network interface. • **Automatically detect** — Media for use with a network interface are automatically detected if available in the network environment of an appliance. • **1000BaseT-FD, 1000Base-HD, ...** — The selected media item is used with a network interface.
Bond enabled	When selected, the currently selected network interface, for example, **eth2**, is configured as a bonded interface that is subordinated to a bonding interface. • **Name** — Specifies the name of the bonding interface.
MTU	Limits the number of bytes in a single transmission unit to the specified value. The default number is 1500. The minimum and maximum numbers depend on whether a network interface is configured under IPv4 or IPv6. • IPv4 — minimum: 576, maximum: 9216 • IPv6 — minimum: 1280, maximum: 9216 If the configured number was set to less than either of these minimum values in an earlier product version, it is now set to 576 under IPv4 and 1280 under IPv6, respectively, by the configuration system on Web Gateway. If it was set to more than the maximum value, it is now set to the default value of 1500. This option is not accessible if the following applies: • This network interface is configured as a bonded interface in a bonding configuration. In this case, **Bond enabled** is selected above.

The following table describes the options provided on the **Advanced** tab when a bonding interface is selected.

Table A-44 Advanced

Option	Definition
Bonding options	Provides options for a bonding interface. • **Mode** — Specifies the mode used to let the bonded network interfaces in the bonding configuration become active. • **Active/Passive** — When selected, only one bonded interface 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. ℹ This mode is referred to in some system messages as *mode 1*. The mode is selected by default. • **802.3ad/LACP** — When selected, all bonded interfaces in the bonding configuration are active. The bonded interface for outgoing traffic is selected according to the configured hash policy. ℹ 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. • **Miimon** — Sets the time interval (in milliseconds) for sending the polling messages of the MII monitoring program. The default interval is 100 milliseconds. • **LACP rate** — Sets the transmission rate for sending LACP-DU data packets in 802.3ad mode. • **Slow** — When selected, data packets are sent every 30 seconds. This transmission rate is selected by default. • **Fast** — When selected, data packets are sent every second. • **Hash policy** — Determines the way that a hash value is calculated for a bonding configuration. • **Layer2** — When selected, a combination of layer 2 values is used 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** — When selected, a combination of layer 2 and layer 3 protocol information is used to calculate the hash.

Network Protection settings

The Network Protection settings are system settings that are used for configuring protective rules for traffic coming in to an appliance from your network.

We recommend configuring Network Protection settings in explicit proxy mode only. You can configure these settings also in the following modes, but you will not receive support when issues occur::

- Proxy HA
- Transparent Router

Network Protection Rules

Settings for configuring network protection rules

Table A-45 Network Protection Rules

Option	Definition
Enable network protection	When selected, the settings configured in the following for network protection are enabled.
Input policy	Lets you select the action taken on incoming traffic. Incoming traffic can either be dropped or accepted.
Allow Ping requests	When selected, the appliance accepts and answers Ping requests.
Exceptions from default policy	Provides a list for entering the network devices that send traffic to an appliance. Traffic from these devices is not handled according to the rules that are currently implemented. When these rules drop incoming traffic, traffic sent from the devices listed here is accepted and vice versa.

The following table describes an entry in the list of exceptions from the default policy.

Table A-46 Exceptions from default policy – List entry

Option	Definition
Device	Specifies the name of a network device that sends traffic to the appliance. Typing * or no input means all devices are covered.
Protocol	Specified the protocol used for sending traffic.
Source	Specifies the IP address or address range of the network device or devices that send traffic to the appliance.
Destination port	Specifies the port on an appliance that is the destination of network traffic.
Comment	Provides a plain-text comment on an exception.

Persistent Data Storage settings

Persistent Data Storage settings are settings for time intervals related to storing data persistently.

Persistent Data Storage is shortly referred to as *PDStorage*.

It enables you to store data beyond any particular transaction that is completed on Web Gateway when an incoming request is processed through all filtering cycles that apply.

When a transaction is completed, values that were retrieved for properties during the transaction are not preserved, but overwritten during the next transaction.

Using PDStorage, you can persistently store data and continue to use it in any following transaction. Data is stored then in a key-value format. You can limit the time for storing the data.

For example, you can store the IP address of a client system that a user sends a request from. When the same user sends another request, you can have a rule that includes suitable PDStorage properties compare the client IP address coming in with this request to the one that is persistently stored.

If the two differ, the rule will, for example, block the request. This way you can restrict web usage for a user to using one particular client system only.

PDStorage Intervals for Synchronisation and Saving in Minutes

Settings for time intervals related to Persistent Data Storage

Table A-47 PDStorage Intervals for Synchronisation and Saving in Minutes

Option	Definition
Save interval	Sets the time (in minutes) that elapses before persistent data is saved again on an appliance.
Enable synchronization of PDStorage data	When selected, persistent data is synchronized according to what you configure for this process.
Interval for sending PDStorage data	Sets the time (in minutes) that elapses before persistent data is distributed again from an appliance to all nodes in a Central Management configuration.
Delay in seconds between the PDStorage messages to be sent	Sets the time (in seconds) that elapses until another PDStorage message follows the message that was sent before it.

PDStorage Memory Management

Setting for the memory size that is available to Persistent Data Storage

Table A-48 PDStorage Memory Management

Option	Definition
Maximum byte size for PDStorage	Limits the size (MiB) of the memory where persistent data is stored.

Port Forwarding settings

The **Port Forwarding** settings are used for configuring rules that let an appliance forward web traffic sent from a port on a particular host to another port.

Port Forwarding

Settings for configuring port forwarding rules

Table A-49 Port Forwarding

Option	Definition
Port forwarding rules	Provides a list of port forwarding rules.

The following table describes an entry in the list of port forwarding rules.

Table A-50 Port forwarding rules – List entry

Option	Definition
Source host	Specifies the IP address of a host that is the source of web traffic in a port forwarding rule.
Bind IP	Specifies the bind IP address.
Target port	Specifies the port that web traffic from the source host is forwarded to.
Destination host	Specifies the IP address of the host that is the destination of web traffic sent from the source host.
Destination port	Specifies the port on the destination host used for listening to web traffic coming in from the source host.
Comment	Provides a plain-text comment on a port forwarding rule.

The **Port Forwarding** settings continue as follows.

Table A-51 Port Forwarding (continued)

Option	Definition
Enable extended connection logging	When selected, all logs for port forwarding are stored on the appliance system under */var/log/mwg_fwd.log*. The logging options that you configure here apply to all port forwarding that performed under the configured port forwarding rules. The stored log files can also be viewed on the user interface under the **Troubleshooting** top-level menu. Select the appliance that you want to view log files for, then select **Log files** and open the **system** folder.
Customize extended logging fields	When selected, the input fields for configuring the type of data that should be logged become accessible.
Log on success	Lets you enter the type of data to be logged when web traffic is successfully forwarded. You can enter one or more of the following data types by typing them in capital letters, separated by commas: PID, HOST, USERID, EXIT, DURATION, TRAFFIC.
Log on failure	Lets you enter the type of data to be logged when forwarding web traffic failed. You can enter one or more of the following data types by typing them in capital letters, separated by commas: HOST, USERID, ATTEMPT. HOST data is logged by default.

Proxies settings

The **Proxies** settings are used for configuring proxies on a Web Gateway appliance.

For more information, see the sections on proxies and their settings in the *McAfee Web Gateway Product Guide*.

Static Routes settings

The **Static Routes** settings are used for configuring routes that always use the same gateway and interface on this gateway when web traffic is routed from an appliance to a particular host.

Static Routes

Settings for static routes under IPv4 or IPv6

Table A-52 Static Routes

Option	Definition
Static routes list	Provides a list of static routes for transmitting web traffic under IPv4 or IPv6.

The following table describes an entry in the list of static routes.

Table A-53 Static routes list – List entry

Option	Definition
Destination	Specifies the IP address and (optionally) net mask of the host that is the destination of a static route.
Gateway	Specifies the IP address of the gateway for routing web traffic from the appliance to a host.
Device	Specifies the interface used on a gateway for a static route.

Table A-53 Static routes list – List entry *(continued)*

Option	Definition
Description	Provides a plain-text description of a static route.
Comment	Provides a plain-text comment on a static route.

Source-based routing

Settings for source-based routing under IPv4 or IPv6

Table A-54 Source-based routing

Option	Definition
Source-based routing for IPv4	When selected, source-based routing is performed under IPv4.
Source-based routing for IPv6	When selected, source-based routing is performed under IPv6.
Static source routing table number	Provides a list of entries for source routing tables that are used to route the traffic that is sent and received through the management user interface.
Source-based routing list for IPv4	Provides a list of routing entries for the traffic that is sent and received through the management user interface. These routing entries are for a network where IPv4 is followed.
Source-based routing list for IPv6	These routing entries are for a network where IPv6 is followed.

The following table describes an entry in the list for static source routing tables.

Table A-55 Static source routing table number – List entry

Option	Definition
Source information to look up routing table	Specifies the source IP address of the traffic that is routed according to the configured static source routing table.
Routing table number	Specifies the number of the routing table for routing the traffic that is sent and received through the management user interface.
Comment	Provides a plain-text comment on a static source routing table.

The following table describes an entry in the list for source-based routing under IPv4.

Table A-56 Source-based routing list for IPv4 – List entry

Option	Definition
Destination	Specifies the IP address range (in CIDR notation) for the destinations of the traffic that is sent through the management network interface.
Routing table number	Specifies the number of the routing table for routing the traffic that is sent and received through the management user interface.
Gateway	Specifies the IP address of the gateway for the traffic that is sent and received through the management network interface.
Device	Specifies the name of the network interface that is configured as the management network interface.
Source IP	Specifies the IP address of the network interface that is configured as the management network interface. This address is the source IP address of the traffic that is routed according to the routing table.
Comment	Provides a plain-text comment on an entry for source-based routing.

The following table describes an entry in the list for source-based routing under IPv6.

Table A-57 Source-based routing list for IPv6 – List entry

Option	Definition
Destination	Specifies the IP address range (in CIDR notation) for the destinations of the traffic that is sent through the management network interface.
Routing table number	Specifies the number of the routing table for routing the traffic that is sent and received through the management user interface.
Gateway	Specifies the IP address of the gateway for the traffic that is sent and received through the management network interface.
Device	Specifies the name of the network interface that is configured as the management network interface.
Source IP	Specifies the IP address of the network interface that is configured as the management network interface. This address is the source IP address of the traffic that is routed according to the routing table.
Comment	Provides a plain-text comment on an entry for source-based routing.

Telemetry settings

The Telemetry settings are used for configuring the collection of feedback data about web objects that are potentially malicious, as well as about policy configuration.

Feedback Settings

Settings for collecting feedback data

You can separately enable or disable each of the following options.

Table A-58 Feedback Settings

Option	Definition
Send feedback to McAfee about system information and suspicious URLs to improve its threat prediction and protection services	When selected, feedback data is collected and sent to special McAfee feedback servers. McAfee collects this data to analyze it and improve the threat prediction and protection features of Web Gateway. For more information, see the *Data Usage Statement*.
Send feedback to McAfee about potentially malicious websites	When selected, relevant data for virus and malware filtering is collected and sent to a special McAfee feedback server.
Send feedback to McAfee about dynamically classified websites	When selected, relevant data for classifying websites is collected and sent to a special McAfee feedback server.
Send feedback to McAfee about policy configuration to improve the product	When selected, relevant data for policy configuration is collected and sent to a special McAfee feedback server.

Further Information

Link to the Data Usage Statement

Table A-59 Further Information

Option	Definition
Data Usage Statement	Provides a link to the data usage statement, which explains: • What McAfee uses collected feedback data for • What data is collected • How data collection can be turned off for different types of data ℹ The data usage statement has also been presented to you at the initial setup of the appliance.

Advanced Settings

Advanced settings for collecting feedback data

Table A-60 Advanced Settings

Option	Definition
Use upstream proxy	When selected, a proxy server is used to send feedback data to McAfee.
IP or name of the proxy	Specifies the IP address or host name of the proxy server.
Port of the proxy	Specifies the port number of the port on the proxy server that listens for requests to send feedback data. The port number can range from 1 to 65635. The default port number is 9090.
User name	Provides the user name that is required for logging on to the proxy server.
Password	Provides the password that is required for logging on to the proxy server. Clicking **Set** opens a window for setting the password.
Choose feedback server	When selected, an IP address and port number can be configured for the server that feedback data is sent to.
IP of the server	Specifies the IP address of the feedback server.
Port of the server	Specifies the port number of the port on the feedback server that listens for requests to send data. The port number can range from 1 to 65635. The default port number is 443.
Port of the server	When selected, feedback-sending activities are logged.

User Interface settings

The **User Interface** settings are used for configuring the local user interface on a Web Gateway appliance. This includes the configuration of ports, the logon page, a certificate for communication under HTTPS, and other items.

UI Access

Settings for configuring access to the interface of an appliance

Table A-61 UI Access

Option	Definition
HTTP connector	Provides options for configuring access to the interface of an appliance under HTTP. • **Enable local user interface over HTTP** — When selected, the HTTP ports that are configured on an appliance for connecting to the interface are enabled. • **HTTP connector** — Specifies an HTTP port for connecting to the interface. You can enter more than one port here, separating entries by commas. Ports can range from 1024 to 65335. Together with a port, you can enter an IP address. This means connecting to the interface of an appliance over this port requires that you specify both the port and this IP address. For example, there are two interfaces for connecting on an appliance with these IP addresses: eth0: 192.168.0.10, eth1: 10.149.110.10 You enter this under **HTTP connector**: `4711, 192.168.0.10:4722` Then connecting to a file server on the appliance over port 4711 is allowed using both IP addresses, whereas connecting over port 4722 requires that IP address 192.168.0.10 is used. Restricting connections in this way might be useful, for example, if you want to set up an intranet. • **Enable REST interface over HTTP** — When selected, you can use the HTTP ports that are configured to connect to the REST interface.
HTTPS connector	Provides options for configuring access to the interface of an appliance under HTTPS. • **Enable local user interface over HTTPS** — When selected, the HTTP ports that are configured on an appliance for connecting to the interface are enabled. • **HTTPS connector** — Specifies an HTTPS port for connecting to the interface. You can enter more than one port here, separating entries by commas. Ports can range from 1024 to 65335. Entering a port together with an IP address can be done in the same way as under **HTTP connector** and has the same meaning. • **Enable REST interface over HTTPS** — When selected, you can use the HTTP ports that are configured to connect to the REST interface. Using the following options, you can specify a protocol and a list of valid ciphers for the HTTPS communication. • **SSL protocol version** — Specifies the version of the SSL protocol that is used for communication with the interface. • **TLS 1.2** • **TLS 1.1** • **TLS 1.0** • **Server cipher list** — Specifies a string of Open SSL symbols used for encrypting communication with the interface.

Table A-61 UI Access *(continued)*

Option	Definition
HTTPS client certificate connector	Provides options for configuring a client certificate connector. • **Enable client certificate authentication** — When selected, client certificate authentication can be performed. • **HTTPS connector for client certificate authentication** — Specifies a port for connecting to the interface when client certificate authentication is performed. You can enter more than one port here, separating entries by commas. Ports can range from 1024 to 65335. Entering a port together with an IP address can be done in the same way as under **HTTP connector** and has the same meaning. • **Redirect target after authentication** — When selected, a request is redirected after client certificate authentication has successfully been performed. • **Redirection host and port** — Specifies the host system and the port on the system that requests are redirected to.
Miscellaneous	Provides miscellaneous options for configuring access to the interface of an appliance. • **Session timeout** — Limits the time (in minutes) that elapses before a session on the interface is closed if no activities occur. The range for the session timeout is 1–99,999 minutes. The timeout is 30 minutes by default.

Login Page Options

Settings for the page that is used to log on to the interface of an appliance

Table A-62 Login Page Options

Option	Definition
Allow browser to save login credentials	When selected, credentials submitted by a user for logging on to the interface are saved by the browser.
Restrict browser session to IP address of user	When selected, a session for working with the interface is only valid as long as the IP address of the client that the user started this session from remains the same.
Let user decide to restrict session for IP address or not	When selected, it is up to the user who started a session for working with the interface whether it should be valid only for the IP address of the client that the session was started from.
Allow multiple logins per login name	When selected, more than one user can log on to the interface under the same user name and password.
Use HTTPOnly session cookies (applet loading may take longer)	When selected, HTTPOnly cookies are used for a session with the user interface.

Table A-62 Login Page Options *(continued)*

Option	Definition
Enable protection against cross-site scripting and clickjacking	When selected, the page used by the administrator for logging on to the interface of a Web Gateway appliance from a browser is protected against a common type of attack. The attack can be performed by combining two methods. Two HTTP headers are added when the page is sent to the browser to prevent these methods from being executed. • **Cross-site scripting** — Malicious JavaScript code is inserted in the page, which is executed when the administrator responds to a prompt on the page, for example, by entering a user name. Adding the following header to messages prevents the execution of this attack: Header name: X-XSS-Protection Header value: 1 • **Clickjacking** — The page is embedded in an iFrame, which can be used to steal the data that is entered on the page. Adding the following header to messages prevents the execution of this attack: Header name: X-Frame-Options Header value: DENY
Maximum number of active applet users	Limits the number of users that can be logged on to the interface at the same time. The maximum number of users is 20 by default.
Login message	Provides the following options for displaying an additional message on the page used for logging on to the interface. You can work with these options if you want to display a message, for example, to comply with internal policies or external regulations. • **Show on login page** — When selected, the text that you type in the **HTML message** field, appears on the logon page. • **HTML message** — The text that you type in this field appears on the logon page.

User Interface Certificate

Settings for a certificate that is used in SSL-secured communication over the HTTPS port for the interface of an appliance.

Table A-63 User Interface Certificate

Option	Definition
Subject, Issuer, Validity, Extensions	Provide information about the certificate that is currently in use.
Import	Opens the **Import Certificate Authority** window for importing a new certificate.
Certificate chain	Displays a certificate chain that is imported with a certificate.

Import Certificate Authority window

Settings for importing a certificate that is used in SSL-secured communication

Table A-64 Import Certificate Authority window

Option	Definition
Certificate	Specifies the name of a certificate file. The file name can be entered manually or by using the **Browse** button in the same line.
Browse	Opens the local file manager to let you browse for and select a certificate file.
Private key	Specifies the name of a private key file. The file name can be entered manually or by using the **Browse** button in the same line. Only keys that are AES-128-bit encrypted or unencrypted keys can be used here.
Browse	Opens the local file manager to let you browse for and select a private key file.
Password	Sets a password that allows the use of a private key.
Import	Opens the **Import Certificate Authority** window for importing a new certificate.
OK	Starts the import process for the specified certificate.
Certificate chain	Specifies the name of a certificate chain file. The file name can be entered manually or by using the **Browse** button in the same line.
Browse	Opens the local file manager to let you browse for and select a certificate chain file. After importing a certificate with a certificate chain, the certificate chain is displayed in the **Certificate chain** field of the **User Interface Certificate** settings.

Memory Settings

Settings for the memory that is available when working with the interface of an appliance

Table A-65 Memory Settings

Option	Definition
Amount of maximum memory available for GUI applet	Limits the amount of memory (in MiB) that is available for the interface applet. The range for the available maximum is 100–999 MiB. The available maximum is 512 MiB by default.
Amount of maximum memory available for MWG UI backend	Limits the amount of memory (in MiB) that is available for the backedn of the interface. The range for the available maximum is 100–9999 MiB. If no value is specified here, the default maximum of 512 MiB is configured.

REST Settings

Settings for configuring use of the REST interface to work with an appliance

Table A-66 REST Settings

Option	Definition
Maximum size of a REST request	Limits the size (in MiB) of a request that is sent to the REST interface. The maximum amount of memory that is available when working with the REST interface is 200 MiB. The maximum size of a request is 2 MiB by default.
Maximum memory per REST session	Limits the amount of memory (in MiB) that is available for a session when working with the REST interface. The maximum amount of memory that is available when working with the REST interface is 200 MiB. The maximum amount of memory for a session is 10 MiB by default.
Maximum number of active REST users	Limits the number of users that can work with the REST interface at the same time. The maximum number of users is 20 by default.

Windows Domain Membership settings

The Windows Domain Membership settings are used for joining an appliance to a Windows domain.

Join Domain

Settings for joining an appliance to a Windows domain

Table A-67 Join Domain

Option	Definition
Windows domain name	Specifies the name of the domain.
McAfee Web Gateway account name	Specifies the name of an account for an appliance.
Overwrite existing account	When selected, an existing account is overwritten.
Use NTLM version 2	When selected, NTLM version 2 is used.
Timeout for requests to this NTLM domain	Limits the time (in seconds) that elapses before processing stops for a request sent from an appliance to a domain controller if no response is received to the specified value.
Wait time for reconnect to domain controller	Specifies the time (in seconds) that elapses before another attempt is made to connect to a domain controller after a previous attempt failed. The allowed range is from 5 to 300 seconds.
Configured domain controllers	Provides a list for entering the domain controllers that an appliance can connect to in order to retrieve authentication information. Entries must be separated by commas.
Number of active domain controllers	Maximum number of configured domain controllers that can be active at the same time The allowed range is from 1 to 10.

Table A-67 Join Domain *(continued)*

Option	Definition
Administrator name	Specifies the logon name of an existing administrator account that has privileges to join an appliance to a domain by creating a machine account in Active Directory. Logon name and password are only used once to create the machine account. They are not stored.
Password	Specifies the password of the existing administrator account.