Quick Configuration Guide

McAfee® Web Gateway

version 6.9
COPYRIGHT
Copyright © 2011 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS
McAfee®, the McAfee logo, Avert, ePO, ePolicy Orchestrator, Foundstone, Global Threat Intelligence, GroupShield, IntruShield, LinuxShield, MAX (McAfee SecurityAlliance Exchange), NetShield, PortalShield, Preventsys, SecureOS, SecurityAlliance, SiteAdvisor, SmartFilter, Total Protection, Type Enforcement, VirusScan, and WebShield are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANTOR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
Introduction

Thank you for selecting McAfee® Web Gateway as your company's web gateway security solution. The goal of this guide is to quickly get the McAfee Web Gateway software running on your system, for use or testing purposes, with minimal configuration.

It provides you with the information needed to complete a number of Initial steps and tells you how to continue the configuration, depending on which components of the software you have licensed:

- URL Filter
- Anti-Malware
- Anti-Virus
- Anti-Spam
- SSL Scanner

Initial steps

The following four initial steps should be completed when you start working with McAfee Web Gateway:

1. Accessing the user interface
2. Changing the password
3. Importing your license
4. Reviewing system alerts

Accessing the user interface

A platform-independent HTML interface, which can be accessed remotely with a Web browser, is provided as user interface for working with McAfee Web Gateway.

Proceed as follows:

1. Enter the address of the server McAfee Web Gateway is running on and the port number of the user interface (the default port number is 9090, which is the same as for the HTTP proxy port):
   - http://localhost:9090/conf — If McAfee Web Gateway is running on the local machine.
   - http://[IP address]:9090/conf — If McAfee Web Gateway is running on another machine.
Initial steps

When using HTTPS-secured connections:

- https://localhost:9091/conf — If McAfee Web Gateway is running on the local machine
- https://[IP address]:9091/conf — If McAfee Web Gateway is running on another machine.

A new certificate is then generated, which is signed by the McAfee Web Gateway Certificate Authority (sha1 fingerprint = 43 80 eb fa 7e 1f 08 51 e3 46 eb f7 ac a6 87 04 87 35 f9 6f).

Note: You can also enter http://-web.washer-/conf in the address field of your client browser, assuming your browser is already configured to use McAfee Web Gateway as an HTTP proxy server.

When you log on to the user interface, the user name is admin and the initial password is webwasher.

Changing the password

To change the password:

1. Go to the tab provided for this purpose under Home > Preferences on the user interface.
2. In the Change Password section of this tab, enter the current password (in this case, webwasher), and then enter your new password twice.

Importing your license

McAfee Web Gateway only works with a valid license, which is stored in the conf directory.

Note: You can also place it somewhere else providing the browser is able to find it there, for example in a directory on the system where the browser is located.

The license key can be easily imported and changed even while McAfee Web Gateway is running, using a link provided under Home > Licenses on the user interface.

Proceed as follows:

1. In the Import License section of this tab, locate your license.
2. Click Browse to browse for the license.
3. Accept the end user license agreement by selecting the corresponding checkbox.
4. Click Activate License.

Note: For customers with NetCache version 5.2 and newer, a special ICAP license is needed to enable this feature on NetCache. The NetCache ICAP license is: NOQPWOJ.

Reviewing system alerts

After importing your license, the Overview tab appears, which is also located under Home.

On this tab, there is a series of system alerts, telling you what needs to be configured before proceeding any further.

Which system alerts are shown depends on the software components you have licensed.
URL Filter

1. In the **System Alerts** section of the **Overview** tab under **Home**, you should see an alert saying that the URL Filter Database must be downloaded.

   Click the link that is provided with this alert.

   This will take you to the **URL Filter** tab under **Configuration > Update Manager**.

2. In the **Manual Update** section of this tab, click **Do it Now**.

   The initial download of the URL Filter Database will take some time. Subsequent updates of the database are, however, incremental and will not take much time.

3. You should also enable the regular automatic update check. By default this is set for every 6 hours.

   After enabling it, click **Apply Changes**.

4. Go to the **Category Actions** tab under **URL Filter > Policy**.

5. On this tab, you can configure your own URL Filtering policy, using pre-configured actions like Block, Allow, Allow on weekends, and others, for categories such as Pornography, Computer Games, Travel, and others.

   After modifying these settings, click **Apply Changes**.

   If you want to use self-configured actions, you can create them under **Configuration > Action Editor**. They will then be available under **Category Actions**.

6. To test whether your category action policy has been implemented, enter known URLs from a blocked category, such as **www.playboy.com**, to ensure they are blocked (assuming you have configured this action on the **Category Actions** tab).

   Be sure to wait until the URL Filter Database has completely downloaded.

---

Anti-Malware

1. On the **Overview** tab under **Home**, download the anti-malware engine by clicking **Anti Virus Engine and Signatures**, which is provided in the **System Summary** section.

   This will take you to the **AV Engine** tab under **Configuration > Update Manager**.

2. In the **Automatic Update** section of this tab, click **Do it Now**.

3. You should also enable the regular automatic update check, by default set for every 90 minutes.

   After enabling it, click **Apply Changes**.

4. Go to the **Proactive Scanning** tab under **Configuration > Update Manager**.

5. In the **Automatic Update** section of this tab, click **Do it Now**.

   This will update the database.

6. You should also enable the regular automatic update check, by default set for every 90 minutes.

   After enabling it, click **Apply Changes**.

7. A new system alert should appear now, saying that encrypted, corrupted, and multi-part archives cannot be scanned for viruses, and allowing these archives poses a security threat.

   **Note**: These archives are currently allowed by default, so they can be scanned by the URL Filter.
8 If you are only running Anti-Malware, you may want to consider using the Archive Handler to block these archives completely.

Click Select blocking actions for these archives.

This will take you to the Archive Handler tab under Common.

9 In the WEB pull-downs of the Archive Handling section of this tab, select Block as action in the lines labeled Encrypted Archive found, Corrupted Archive found, and Multi-part Archive found.

Under MAIL, select Replace and Quarantine for these three types of archives.

Then click Apply Changes.

10 Make sure Proactive Scanning is enabled.

It is enabled if the checkbox on the Proactive Scanning button is selected. This button is located in the navigation area on the left side of the Anti Malware top-level tab.

Note: Proactive Scanning is enabled by default.

11 To test whether virus protection is working properly, go to http://www.eicar.org, where you can download the Eicar anti-virus test files.

These files are for test purposes only and contain a virus “signature” that all virus scanners will detect as Eicar test files.

These files are not real viruses and do not cause any harm, should they pass through (if the virus signature download has not finished before you attempt to download the files).

12 Click the AntiVirus testfile eicar.com link on the left-hand side of the page and review this page.

13 Download a test virus.

By selecting the zipped Eicar virus file (eicar.zip) and the nested archive file (eicar8.zip), you can test how the virus scanner extracts archives.

If McAfee Web Gateway has successfully blocked this virus, a virus alert block message will appear. If it doesn't work, please clear your cache before trying again.

You should also receive a virus alert notification message, indicating that everything is working properly.

---

**Anti-Virus**

1 On the Overview tab under Home, download the AV engines you have licensed by clicking the Anti Virus Engine and Signatures link, which is provided in the System Summary section.

This will take you to the AV Engine tab under Configuration > Update Manager.

2 In the Automatic Update section of this tab, click Do it Now.

3 You should also enable the regular automatic update check, by default set for every 90 minutes.

After enabling it, click Apply Changes.

4 Go to the Proactive Scanning tab under Configuration > Update Manager. In the Automatic Update section of this tab, click Do it Now.

This will update the database.

5 You should also enable the regular automatic update check, by default set for every 90 minutes.

After enabling it, click Apply Changes.
A new system alert should appear now, saying that encrypted, corrupted and multi-part archives cannot be scanned for viruses, and allowing these archives poses a security threat.

**Note:** These archives are currently allowed by default, so they can be scanned by the URL Filter.

If you are only running Anti-Virus, you may want to consider using the Archive Handler to block these archives completely.

Click **Select blocking actions for these archives** link.

This will take you to the **Archive Handler** tab under **Common**.

From the **WEB** pull-downs of the **Archive Handling** section of this tab, select **Block** as action in the lines labeled **Encrypted Archive found**, **Corrupted Archive found**, and **Multi-part Archive found**.

Under **MAIL**, select **Replace and Quarantine** for these three types of archives.

Then click **Apply Changes**.

Make sure **Proactive Scanning** is enabled.

It is enabled if the checkbox on the **Proactive Scanning** button is selected. This button is located in the navigation area on the left side of the **Anti Malware** top level tab.

**Note:** Proactive Scanning is enabled by default.

To test whether virus protection is working properly, go to **http://www.eicar.org**, where you can download the Eicar anti-virus test files.

These files are for test purposes only and contain a virus “signature” that all virus scanners will detect as Eicar test files.

These files are not real viruses and do not cause any harm, should they pass through (if the virus signature download hasn’t finished before you attempt to download the files).

Click the **AntiVirus testfile eicar.com** link on the left-hand side of the page and review this page.

Download a test virus.

By selecting the zipped Eicar virus file (*eicar.zip*) and the nested archive file (*eicar8.zip*), you can test how the virus scanner extracts archives.

If McAfee Web Gateway has successfully blocked this virus, a virus alert block message will appear. If it doesn’t work, please clear your cache before trying again.

You should also receive a virus alert notification message, indicating that everything is working properly.

Included with the Anti-Spam component are also URL filtering methods, which require the implementation of the URL Filter Database.

Please download this database – instructions can be found in the **URL Filter** section of this document.

To assist you with the configuration of the e-mail gateway, a Spam Filter wizard is provided. If you want to use this wizard, go to **Configuration > Wizards > Spam Filter Setup**.
Alternatively, you can configure spam filtering in the following way:

1. In the System Alerts section of the Overview tab under Home, you should see an alert saying that the spam filter is activated.

Furthermore, it asks you to check if you also want to enable the e-mail gateway. Click the link that is provided with this alert.

This will take you to the Gateway Settings tab under Proxies > E-Mail Gateway.

2. Enable McAfee Web Gateway to run as an e-mail gateway by selecting the checkbox on the E-Mail Gateway button. This button is located in the navigation area to the left of the Gateway Settings tab.

Then click Apply Changes.

3. After installation, McAfee Web Gateway will only accept e-mails from the local host (IP address 127.0.0.1). This means that additional rules need to be set up so that users can send and receive e-mails in the usual way.

For example, you can configure McAfee Web Gateway to deliver all e-mails that are going out from your corporate network, but accept only incoming e-mails addressed to the employees of your company.

Incoming e-mails addressed to any other recipients will then be blocked to prevent spammers from using McAfee Web Gateway as a relay server for distributing spam.

To set up the corresponding rules, first go to the IP Networks tab under Proxies > Relay Protection.

4. On this tab, there is an Add Rule section for entering and adding rules and a Current Networks section for listing and displaying all the rules that have been added so far.

Using the Add Rule section, add a rule to specify the IP address range of your local network, Furthermore, add a rule to specify the IP address range of the Internet that you want to allow to send e-mails to the local network later on.

Proceed as follows:

a. For the first rule, enter: localnetwork = 192.168.0.1 - 192.168.0.200

b. Click Add Last.

This will add the rule to the list of rules displayed under Current Networks.

c. For the second rule, enter: internet = *

d. Click Add Last.

This will add the rule to the list of rules displayed under Current Networks.

Note: The local network rule excludes the addresses specified there from the range of addresses specified by the general wildcard in the Internet rule, so in effect the Internet rule will apply to any address that is not within your local network.

5. Then set up rules for the domains that e-mails may be sent to from within the address ranges specified under IP Networks.

Go to the Allowed Domains tab under Proxies > Relay Protection.

6. On this tab, there is an Add Rule section for entering and adding rules and a Current Rules section for listing and displaying all the rules that have been added so far.

Using the Add Rule section, add a rule to specify the domains that senders within the address range of your local network may send e-mails to.
Furthermore, add a rule to specify the domains that senders within the Internet address range specified on the IP Networks tab on may send e-mails to.

Proceed as follows:

a For the first rule, enter: `localnetwork = *`

b Click Add Last.

This will add the rule to the list of rules displayed under Current Rules.

The meaning of the rule is that senders within the address range of your local network, which you specified on the IP Networks tab, may send e-mails to any domain within the Internet.

c For the second rule, enter: `internet = <yourcompanydomain>`

where `yourcompanydomain` is a placeholder for your actual corporate domain name.

d Click Add Last.

This will add the rule to the list of rules displayed under Current Rules.

The meaning of this rule is that senders within the address range of the Internet you specified on the IP Networks tab may send e-mails only to recipients within your corporate domain, and McAfee Web Gateway will not relay e-mails sent from the Internet to any other recipients.

This will prevent spammers from using McAfee Web Gateway as a relay server for distributing spam.

7 To test if the rules you have just set up work, open a Telnet client and establish a connection to the e-mail gateway that is provided by McAfee Web Gateway.

On the Telnet client, enter the following commands:

telnet `<Webwasher IP>` `<port number of the Webwasher e-mail gateway>`

This port number is usually 25. A 220 answer should appear.

Helo `<some random characters>`

A 250 OK answer should appear.

mail from `<employee@yourcompanydomain>`

A 250 OK answer should appear.

rcpt to `<employee@yourcompanydomain>`

A 250 OK answer should appear.

data `<some random characters>`

A 250 Message accepted for delivery should appear. This would mean that everything is working according to the rules you set up.

QUIT

To close the connection.

8 Go back to the Overview tab under Home.

In the System Alerts section, you should see another alert, saying that the Real-Time Blackhole Lists spam filtering method cannot operate without further setup.

9 Click the link that is provided together with this alert.

This will take you to the RBL Settings tab under Anti Spam > Policy-Independent.
10 On this tab, specify the appropriate settings, which you make take from the RBL server list provided by McAfee Web Gateway.

To view this list, click the question mark in the top right corner of the tab.

This will launch the corresponding online-help page, where you will find a link that takes you to the list.

11 If you do not want to use the RBL method, go to the **Spam Filtering Methods** tab under **Anti Spam > Policy-Independent**

12 Disable the method by deselecting the checkbox next to the heading of the **Real-Time Blackhole Lists** section.

Then click **Apply Changes**.

13 Go back to the **Overview** tab under **Home**.

In the **System Alerts** section, you should finally see an alert, saying that there has been no update check of the Spam Filter Database for at least 3 days.

14 The Anti-Spam component ships with a default database, but you can update to a newer one.

To do this, click the link that is provided together with the alert.

This will take you to the **Spam Filter** tab under **Configuration > Update Manager**.

15 In the **Manual Update** section of this tab, click **Do it Now**.

16 You should also enable the regular automatic update check, by default set for every 15 minutes.

After enabling it, click **Apply Changes**.

17 For further testing, you can check existing e-mail messages to see whether a “spam-likelihood” header was attached to some of them by McAfee Web Gateway.

---

**SSL Scanner**

1 By default, the SSL Scanner component is already enabled after installation.

To test if it is working properly, enter the following URL in a browser window:

https://www.lufthansa.de/

You should receive a **Server Certificate Verification Failed** notification since the correct domain is **.com**, and therefore **.de** does not match the certificate.

**Note:** The SSL Scanner is by default configured to block certificates that do not match the domain name, are unsigned, or not trusted.

2 Under McAfee Web Gateway, the root Certificate Authority (CA), which is a trusted agency that assigns certificates of authentication to Web servers, should be the Webwasher root CA. To see if this is actually so, click the lock icon at the bottom of your browser.

The certificate window will appear to confirm that Webwasher is in fact this root CA.

---

**Fine-tuning McAfee Web Gateway**

McAfee Web Gateway is now initially configured. You can fine-tune the configuration via the user interface.

Please refer to the user documentation for more details about the configuration features provided by McAfee Web Gateway.