

Quick Start Guide

McAfee Web Gateway

version 7.2

This Quick Start Guide provides high-level instructions for setting up a McAfee[®] Web Gateway appliance.

Before you begin, be sure to read the release notes, which provide information on known issues. The release notes are available at mysupport.mcafee.com.

Refer to the McAfee Web Gateway Product Guide for further information.

1 Check your shipment

Make sure you received the items needed for the setup:

- McAfee Web Gateway appliance (models vary)
- Power cord
- Network cables
- USB-PS/2 adapter cable (if you use a PS/2 keyboard for the initial configuration)

2 Gather necessary materials

You must provide the following:

- Standard VGA monitor and PS/2 or USB keyboard or serial console
- Administration system with:
 - Microsoft Windows or Linux operating system
 - Java Runtime Environment (JRE) version 1.6 or later
- Microsoft Internet Explorer version 6.0 or later *or* Mozilla Firefox version 2.0 or later
- Network cables for the administration system





3 Review the initial configuration settings

The following settings are implemented by default during the initial configuration of an appliance:

٠

•

- Primary network interface: eth0
- Autoconfiguration with DHCP: yes
- Host name: mwgappl
- Root password: <none>
- Remote root logon with SSH: on Default gateway: <configured by DHCP>
- DNS server: <configured by DHCP>

If you want to implement your own settings, use the configuration wizard (see steps 4 and 5).

4 Install the appliance software

- a Connect the appliance to power and the network.
- **b** Connect a monitor and keyboard or a serial console to the appliance.
- **c** Turn on the appliance.

The installation menu appears.

d Select an installation mode, then press Enter.

The appliance software is installed on the appliance.

- e Complete the installation:
 - If you have selected a mode without the configuration wizard, confirm when prompted.

The appliance runs with default initial configuration settings.

• If you have selected a mode with the configuration wizard, confirm when prompted.

Implement your own initial configuration settings (see step 5).

After the installation, each network interface of the appliance has a port assigned to it, for example, eth0 or eth1. For these port assignments, see the *McAfee Web Gateway Product Guide*.





5 Implement your own initial configuration settings

Perform this step only if you have selected an installation mode with the configuration wizard to implement your own initial configuration settings.

When the appliance software is installed, the configuration wizard appears.

- **a** Use the wizard windows to configure the following:
 - Primary network interface
 - IP address, entered manually or configured dynamically by DHCP
 - Host name
 - DNS server
- **b** Review the summary that is displayed after configuring the DNS server.
 - If you approve of the summary, confirm and configure the remaining settings:
 - Root password
 - Remote logon with SSH

The initial configuration is completed with your settings and the IP address is displayed.

Continue with step 6.

• If you need to make changes, click **Cancel** and return to substep a.

6 Log on to the user interface of the appliance

a Open the browser of your administration system and go to:

http://<ip address>:4711

or https://<ip address>:4712

using the IP address from the initial configuration.



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

A logon window opens.

b Enter admin as the user name and webgateway as the password.

After a successful logon, the user interface appears and displays the policy creation wizard.



ethO	driver:e1000	mac:08:00:27:00:75:70
etht	driver:e1000	mac:08:00:27:9a:d3:d2
eth2:	driver:e1000	mac:08:00:27:03:cd:53
eth3.	driver:e1000	mac:08:00:27:66:12:8f

7 Implement an initial web security policy

Do one of the following to implement an initial web security policy:

• Follow the policy creation wizard. When you are done, click **Finish**.

A system of web security rules and filtering lists is implemented, based on your selections.

• Click Default.

The default system of web security rules and filtering lists is implemented.



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

8 Import a license

- a Select Configuration | Appliances.
- b On the appliances tree, select the appliance name and click License.
- c Under Import License, click end user license agreement and review the agreement. If you agree to it, select the checkbox that is provided.
- d Click Browse, locate and select your license file, and click Activate.

The license is imported and license information appears.

After importing the license, an automatic update of virus signatures and other filter information begins. It can take several minutes.

During the update, functions that require updated information, such as virus and malware filtering, are not yet available, which means that requests to access web objects are blocked by the web security rules.

For more information on how to administer an appliance on the user interface, see the online Help and the *McAfee Web Gateway Product Guide*.

Copyright © 2012 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

700-3874A00



Commercial	acion	Europe	our location		
Financial		North Am	North America		
Government		Asia-Paci	Asia-Pacific		
Health Care		South or	South or Central America		
Manufacturing					
School or University					
These selections impor filters, select your org	t common whitelist anization's basic lev	s and recommended vel of restriction.	blocking lists. To cr	eate network traffic	
These selections impor filters, select your org Select a basic level	t common whitelist anization's basic lev of permission o	s and recommended rel of restriction. r restriction	blocking lists. To cr	eate network traffic	
These selections impor filters, select your org Select a basic level	t common whitelist anization's basic lev of permission o	s and recommended rel of restriction. r restriction	blocking lists. To cr	eate network traffic	
These selections impor fikers, select your org Select a basic level	t common whitelist anization's basic lev of permission or Permissive	s and recommended rel of restriction. r restriction	blocking lists. To cr I Restrictive	eate network traffic	
These selections impor filters, select your org Select a basic level	t common whitelist anization's basic lev of permission of Permissive e the documentatic	s and recommended rel of restriction. r restriction United	blocking lists. To cr I Restrictive	eate network traffic	
These selections impor filters, select your org Select a basic level Very Permissive For more guidance, se	t common whitelist anization's basic lev of permission of Permissive e the documentation	s and recommended vel of restriction. r restriction Limited	blocking lists. To cr I Restrictive	eate network traffic	
These selections impor filters, select your org Select a basic level Very Permissive For more guidance, se After this, browse you	t common whitelist anization's basic lev of permission of Permissive e the documentation r Rule Sets for add	s and recommended rel of restriction. r restriction United on. Itional rules to enable	I Restrictive	eate network tr	
e selections impor , select your org ct a basic level y Permissive ore guidance, se this, browse you ibing which user i	t common whitelist anization's basic lev of permission of Permissive e the documentation r Rule Sets for add groups or addresse	s and recommended rel of restriction. r restriction United on. litional rules to enables are Teachers vers	blocking lists. To cr Restrictive le. Populate a rule's us Students - and e	eate network traffic i Very Restrictive alsts - for example, enable the rule.	

Web Gateway Policy Creation