



Installation Guide  
Revision A

McAfee Web Gateway 7.5.2

## **COPYRIGHT**

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, [www.intelsecurity.com](http://www.intelsecurity.com)

## **TRADEMARK ATTRIBUTIONS**

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

## **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 GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY 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.

# Contents

<b>Preface</b>	<b>5</b>
About this guide . . . . .	5
Audience . . . . .	5
Conventions . . . . .	5
Find product documentation . . . . .	6
<b>1 Introduction</b>	<b>7</b>
Main functions of Web Gateway . . . . .	7
Setup procedures for Web Gateway . . . . .	8
<b>2 Setting up Web Gateway</b>	<b>9</b>
High-level steps for setting up Web Gateway . . . . .	9
Verify the requirements . . . . .	10
Review the default initial configuration settings . . . . .	12
Set up a physical appliance with pre-installed software . . . . .	12
Set up a physical appliance with downloaded software . . . . .	12
Download the software for a physical appliance . . . . .	13
Install the downloaded software on a physical appliance . . . . .	13
Set up a virtual appliance . . . . .	14
Download the software for a virtual appliance . . . . .	14
Install the downloaded software on a virtual appliance . . . . .	15
Virtual machine settings . . . . .	15
Implement the initial configuration settings . . . . .	17
Implement the default initial configuration settings . . . . .	17
Implement your own initial configuration settings . . . . .	17
Log on to the user interface . . . . .	18
Work with the setup wizard . . . . .	18
Activate the product . . . . .	19
Configure more initial settings . . . . .	20
Solve problems with connecting to the download servers . . . . .	21
Activate Web Gateway with a temporary license key . . . . .	21
Re-image an appliance . . . . .	22
Default serial system console settings . . . . .	23
Port assignments on a physical appliance . . . . .	23
Port assignments on the new generation appliance models . . . . .	23
Port assignments on the older appliance models . . . . .	25
Memory upgrade . . . . .	27
Purchase Dell memory modules . . . . .	28
Get information on how to install memory modules . . . . .	28
<b>3 Installing a PCI card</b>	<b>31</b>
Supported fiber NICs . . . . .	31
1GbE fiber NIC . . . . .	32
10GbE fiber NIC . . . . .	33
Supported copper NICs . . . . .	35

1GbE copper NIC . . . . .	35
Supported HSM cards . . . . .	36
Install a PCI card . . . . .	37
<b>4 Installing hardware administration tools</b>	<b>39</b>
Tools for administering the Web Gateway hardware . . . . .	39
Install the Platform Confidence Test tool . . . . .	40
Run a hardware test with the Platform Confidence Test tool . . . . .	40
Configure the Remote Management Module . . . . .	41
Install the Active System Console . . . . .	42
Enable the SNMP Subagent . . . . .	42
<b>5 Installing Web Gateway on a blade server</b>	<b>45</b>
Supported blade servers and enclosures . . . . .	45
Installing the blade server system . . . . .	45
Preparing the installation of the blade server system . . . . .	46
Install the blade server system . . . . .	46
Network setup for Web Gateway on a blade server . . . . .	51
Proxy HA on a blade server . . . . .	51
Proxy with external load balancing on a blade server . . . . .	52
Transparent modes on a blade server . . . . .	53
Port assignments on a blade server . . . . .	54
<b>Index</b>	<b>57</b>

# Preface

This guide provides the information you need to work with your McAfee product.

## Contents

- ▶ *About this guide*
- ▶ *Find product documentation*

---

## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

## Audience





McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

## Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
<b>Bold</b>	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	<b>Note:</b> Additional information, like an alternate method of accessing an option.
	<b>Tip:</b> Suggestions and recommendations.
	<b>Important/Caution:</b> Valuable advice to protect your computer system, software installation, network, business, or data.
	<b>Warning:</b> Critical advice to prevent bodily harm when using a hardware product.

---

## Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

### Task

- 1 Go to the **Knowledge Center** tab of the McAfee ServicePortal at <http://support.mcafee.com>.
- 2 In the **Knowledge Base** pane, click a content source:
  - **Product Documentation** to find user documentation
  - **Technical Articles** to find KnowledgeBase articles
- 3 Select **Do not clear my filters**.
- 4 Enter a product, select a version, then click **Search** to display a list of documents.

# 1

## Introduction

McAfee® Web Gateway (Web Gateway) is a web security product that protects your network against threats arising from the web such as viruses and other malware, inappropriate content, data leaks, and related issues. It also ensures regulatory compliance and a productive work environment.

Web Gateway runs as an appliance that connects your network to the web, filtering the traffic that goes out and comes in. Malicious and inappropriate content is blocked, while useful matter is allowed to pass through.

The filtering process is controlled by web security rules that you can configure in a highly flexible manner to let them suit the needs of your network.

### Contents

- ▶ *Main functions of Web Gateway*
- ▶ *Setup procedures for Web Gateway*

---

## Main functions of Web Gateway

Filtering web traffic is a complex process. The main functions of Web Gateway contribute to this process in different ways.

- **Intercepting and transmitting web traffic** — The proxy functions of a Web Gateway appliance intercept requests that users of your network send to the web, and depending on the filtering results, transmit these requests to their destinations. Responses that the destinations send to your network are also intercepted and filtered.
- **Authenticating users** — The authentication functions filter the users of your network, applying different authentication methods to give you control over who is allowed to access the web from inside your network.
- **Filtering web objects** — The web filtering functions filter objects, performing different kinds of filtering, such as virus and malware filtering, URL filtering, media type filtering, or application filtering, to cover all kinds of threats that arise from the web.
- **Monitoring the filtering process** — A comprehensive overview of the filtering process is provided by the monitoring functions, which include a dashboard for alerts and status information, as well as logging, tracing, and troubleshooting functions.

---

## Setup procedures for Web Gateway

Procedures for setting up a Web Gateway appliance differ, depending on the platform you want to run it on and on the way you obtain the appliance software and install it on the platform.

You can set up Web Gateway in the following ways:

- **Physical appliance**

When you run Web Gateway as a physical appliance, you set it up on a hardware platform. The appliance software is available in the following ways:

- **Pre-installed software** — When you purchase a new hardware platform for Web Gateway, the appliance software is pre-installed on this platform.
- **Downloaded software** — If you do not want to use the pre-installed software, you can download it in ISO or USB format from the McAfee Content & Cloud Security Portal and install it.

- **Virtual appliance**

When you run Web Gateway as a virtual appliance, you set it up on a virtual machine that you create on a suitable host system.

You can download the appliance software in ISO format from the McAfee Content & Cloud Security Portal and install it.



# 2

## Setting up Web Gateway

To set up Web Gateway, you need to complete several activities, such as checking your installation materials, configuring initial settings, and logging on to the user interface.

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

When the installation is completed and you log on to the user interface for the first time, you also need to import a license and activate the product.

### Contents

- ▶ *High-level steps for setting up Web Gateway*
- ▶ *Verify the requirements*
- ▶ *Review the default initial configuration settings*
- ▶ *Set up a physical appliance with pre-installed software*
- ▶ *Set up a physical appliance with downloaded software*
- ▶ *Set up a virtual appliance*
- ▶ *Implement the initial configuration settings*
- ▶ *Log on to the user interface*
- ▶ *Work with the setup wizard*
- ▶ *Activate Web Gateway with a temporary license key*
- ▶ *Re-image an appliance*
- ▶ *Default serial system console settings*
- ▶ *Port assignments on a physical appliance*
- ▶ *Memory upgrade*

---

## High-level steps for setting up Web Gateway

To set up a Web Gateway appliance, complete the following high-level steps.

### Task

- 1 Verify the requirements for the setup.
- 2 Review the default initial configuration settings.

- 3 Install the appliance software.
  - When setting up Web Gateway as a physical appliance with pre-installed software, connect and turn on the appliance.
  - When setting up Web Gateway as a physical appliance with downloaded software:
    - Download the software and copy it to some installation media.
    - Connect the appliance, insert the installation media, and turn on the appliance.
    - Work with the Boot Manager to install the software.
  - When setting up Web Gateway as a virtual appliance:
    - Download the software and copy it to some installation media.
    - Insert the installation media into a suitable host system.
    - Create a virtual machine on the host system.
    - Start the new virtual machine.
- 4 Implement the initial configuration settings.
- 5 Log on to the user interface.
- 6 Review online documents and import a license.
- 7 Activate the product.

After completing the setup, you can work with the user interface of Web Gateway to perform more administration activities.



For information on how to upgrade Web Gateway, see the release notes that are provided with each new product version.

---

## Verify the requirements

Before you set up Web Gateway as a physical or virtual appliance, make sure that you have available what is needed.

### Requirements for setting up a physical appliance

To set up a physical appliance, the following is required:

- Items that were shipped to you:
  - Hardware platform (models vary) with appliance software



The recommended minimum memory size on a hardware platform is 8 GB. If you are using an older model with less than this size, you can upgrade. See *Memory upgrade*.

- Power cord
- Network cables
- USB-PS/2 adapter cable (if you use a PS/2 keyboard for the initial configuration)



Installation media (CD/DVD and USB drive) with the appliance software were also shipped to you. They are not required for the setup, but you can use them for re-imaging the appliance.

- Items that you must provide:
  - Standard VGA monitor and PS/2 keyboard  
or serial system console
  - Administration system with:
    - Windows or Linux operating system
    - Oracle Java Runtime Environment (JRE), version 1.6, also referred to as *Java 6*, or later  
JRE is required for running the user interface.



The current version of Web Gateway, version 7.5.1, is the last main version to support JRE, version 1.6 (Java 6). Web Gateway, version 7.5.2, will require JRE, version 1.7 or 1.8 (Java 7 or 8).

As support for Java 7 will also terminate soon, we encourage you to start using Java 8 now if you are not using it already.

- Microsoft Internet Explorer, version 6.0 or later  
or Mozilla Firefox, version 2.0 or later
- Network cables for the administration system

### Requirements for setting up a virtual appliance

To set up a virtual appliance, the following is required:

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



If you are running version 5.5, make sure that you use update 2 or a later update of this version.

- Virtual machine host system with the following specifications:
  - CPU — 64-bit capable
  - Virtualization extension — VT-x/AMD-V
- Virtual machine with the specifications shown in the following table.



Specifications differ depending on what you are using a virtual appliance for.

**Table 2-1 Specifications for a virtual machine**

Use	Memory (RAM in GB)	Hard disk space (in GB)	CPU cores
Functional testing (one user) or Central Management console (no traffic)	4	80	2
Production (minimum)	16	200	4
Production (recommended)	32	500	at least 4

## Review the default initial configuration settings

You can set up an appliance with default initial configuration settings or implement your own settings, using the configuration wizard that appears during the process.

The following table shows the default settings.

**Table 2-2 Default initial configuration settings**

Parameter	Value
Primary network interface	eth0
Autoconfiguration with DHCP	yes
Host name	mwgappl
Root password	webgateway
Remote root logon with SSH	on
Default gateway	<configured by DHCP>
DNS server	<configured by DHCP>

## Set up a physical appliance with pre-installed software

On a newly purchased hardware platform, the appliance software is pre-installed. Connect the appliance and turn it on.

### Task

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

The configuration wizard appears.

You can now work with the configuration wizard to implement the initial configuration settings.

### See also

[Default serial system console settings on page 23](#)

[Port assignments on a physical appliance on page 23](#)

## Set up a physical appliance with downloaded software

When setting up a physical appliance, you can install software that you downloaded from the McAfee Content & Cloud Security Portal.

### Tasks

- [Download the software for a physical appliance on page 13](#)  
You can download different versions of the appliance software in ISO or USB format.
- [Install the downloaded software on a physical appliance on page 13](#)  
To install the downloaded software on a physical appliance, connect the appliance, turn it on, and work with the Boot Manager.

## Download the software for a physical appliance

You can download different versions of the appliance software in ISO or USB format.


### Task

- 1 Use a browser to go to the McAfee Content & Cloud Security Portal at <https://contentsecurity.mcafee.com/>
- 2 Submit your user name and password.
- 3 Beginning on the home page of the portal, select **Software | McAfee Web Gateway 7 | Download**.  
A page with software versions in ISO and USB format appears.
- 4 Click the icon for the exact software version you want to download.  
A download window opens.
- 5 Select the option for storing a file and click **OK**.  
The software is downloaded and stored within your file system.
- 6 Copy the downloaded software to a CD/DVD or a USB drive to have it available for installation.

## Install the downloaded software on a physical appliance

To install the downloaded software on a physical appliance, connect the appliance, turn it on, and work with the Boot Manager.

### Task

- 1 Connect the appliance to power and the network.
  - 2 Connect a monitor and keyboard or a serial system console to the appliance.
  - 3 Insert the CD/DVD or the USB drive with the downloaded software.
  - 4 Turn on the appliance.  
The installation begins.
  - 5 During the initial phase, select the installation device:
    - If your appliance hardware model is Web Gateway (WBG) 4500B, 5000B, or 5500B:
      - Press **F6** to enter the Boot Manager.
      - Select the drive for the CD/DVD or USB format, then press **Enter**.
    - If your model is Web Gateway (WBG) 4000B:
      - Press **F2** to enter the BIOS setup menu.
      - Select **Boot Options** and click **Hard Disk Order**.
      - Select the option that assigns the CD/DVD or USB drive the highest priority.
      - Click the **Exit** tab.
      - Select **Discard Changes**.
-  Do not use the **Discard Changes and Exit** option here.
- Select **Boot Manager** and select the drive for the CD/DVD or USB format. Then press **Enter**.

- If your model is not specified:
  - Press **F11** to enter the Boot Manager.
  - Select the drive for the CD/DVD or USB format, then press **Enter**.

The installation menu appears on the monitor.

- 6 Select an installation mode, then press **Enter**.



Help text is displayed for a selected mode below the menu.

The downloaded software is installed on the appliance. When this installation is completed, the configuration wizard appears.

You can now work with the configuration wizard to implement the initial configuration settings.

### See also

[Default serial system console settings on page 23](#)

[Port assignments on a physical appliance on page 23](#)

---

## Set up a virtual appliance

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

### Tasks

- [Download the software for a virtual appliance on page 14](#)  
You can download different versions of the appliance software in ISO format.
- [Install the downloaded software on a virtual appliance on page 15](#)  
To install the downloaded software on a virtual appliance, insert the CD/DVD with the software in a suitable host system, create a virtual machine on this system, and start the virtual machine.

## Download the software for a virtual appliance

You can download different versions of the appliance software in ISO format.

### Task

- 1 Use a browser to go to the McAfee Content & Cloud Security Portal at <https://contentsecurity.mcafee.com/>.
- 2 Submit your user name and password.
- 3 Beginning on the home page of the portal, select **Software | McAfee Web Gateway 7 | Download**.  
A page with software versions in ISO and USB format appears.
- 4 Click the ISO icon for the exact software version you want to download.  
A download window opens.
- 5 Select the option for storing a file and click **OK**.  
The software is downloaded and stored within your file system.
- 6 Copy the downloaded software to a CD/DVD to have it available for installation.

## Install the downloaded software on a virtual appliance

To install the downloaded software on a virtual appliance, insert the CD/DVD with the software in a suitable host system, create a virtual machine on this system, and start the virtual machine.

### Task

- 1 Connect a keyboard and monitor to a suitable host system.
- 2 Insert the CD/DVD with the appliance software.
- 3 Using your VMware, create a virtual machine on the host system.
- 4 Start the new virtual machine.

The appliance software is installed on the virtual machine. When this installation is completed, the configuration wizard appears on the monitor of the host system.

You can now work with the configuration wizard to implement the initial configuration settings.

If your VMware type is ESXi and you are running a Vsphere client, you can use the following methods to make the appliance software available on the host system:



- Insert a CD/DVD with the appliance software into the host system (as was already described)
- Store the appliance software on a local disk or the datastore of the host system
- Store the appliance software on a USB drive and insert it into the host system

## Virtual machine settings

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

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





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

**Table 2-3 Virtual machine settings**

Option	Definition
Configuration type	Typical   Advanced (recommended)
Installation mode	Install from disk   ISO image (required)   Install later
Operating system	Linux 64 bit, version 2.6

**Table 2-3 Virtual machine settings** (continued)

Option	Definition
Memory	<p>32 GB (recommended, for more information, see <i>Verify the requirements</i>)</p> <p>Starting with version 4.1, VMware ESXi, which is one of the supported VMware types for a virtual Web Gateway appliance, includes some optimizations known as <i>NUMA optimizations</i>.</p> <p>A host system for virtual machines that runs this VMware is also referred to as a <i>NUMA node</i>. Memory must then be allotted to a virtual machine in relation to the memory that is available on a NUMA node, otherwise you might experience a severe impact on performance.</p> <p> For example, if you set up three virtual machines on one NUMA node and configure the same number of processors (also known as <i>CPU cores</i>) for each virtual machine, you should not allot more than one third of the memory that is available on the NUMA node to each virtual machine.</p> <p>Best results are achieved, however, if you run one virtual machine on one NUMA node.</p> <p>Make sure that you also reserve a certain amount of memory for the NUMA node (the host system).</p>
Hard-disk space	500 GB (recommended, for more information, see <i>Verify the requirements</i> )
Number of processors	<p>1   2   4 (recommended, for more information, see <i>Verify the requirements</i>)   ...</p> <p>The number of processors (also known as <i>CPU cores</i>) that are provided for selection depends on the equipment of the host system that is used for setting up the virtual appliance.</p> <p>When virtual machines are set up on a host system that runs ESXi VMware, version 4.1 or later, with NUMA optimizations, see also under <i>Memory</i>, CPU cores should be configured in relation to what is allowed on a <i>NUMA node</i> (a host system).</p> <p>The number of CPU cores that you configure for a virtual machine should be multiples or divisors of the number of CPU cores that fit in with the size of a NUMA node.</p> <p> For example, if the size of a NUMA node is sufficient for running six CPU cores, you should configure virtual machines with two, three, or six cores (if you are only using one node), or with 12, 18, 24, and so on (if you are using multiple nodes).</p> <p>Best results are achieved, however, if you run one virtual machine on one NUMA node.</p>
Network connection mode	Bridged (recommended)   NAT   ...
CD/DVD drive with assigned ISO image	<drive name>/<name of the ISO image>
Network interface card type	E1000   VMXNET 3 (recommended)
SCSI controller (for some ESX versions)	BusLogic SCSI (not supported in a 64-bit environment)   LSI Logic Parallel (default)   LSI Logic SAS   VMware PV SCSI (recommended)



## Implement the initial configuration settings

Work with the configuration wizard to implement the default or your own initial configuration settings on an appliance.

### Tasks

- *Implement the default initial configuration settings on page 17*  
To implement the default initial configuration settings, work with the wizard to configure a root password and remote root logon, but leave the remaining settings unchanged.
- *Implement your own initial configuration settings on page 17*  
To implement your own initial configuration settings, follow the instructions of the wizard.

## Implement the default initial configuration settings

To implement the default initial configuration settings, work with the wizard to configure a root password and remote root logon, but leave the remaining settings unchanged.

### Task

- 1 Press **Esc** in response to all prompts of the configuration wizard until the root password is configured.
- 2 When asked for the root password, enter and repeat it, then confirm it with **OK**.
- 3 When asked to allow remote root logon with SSH, click **Yes** or **No**.

When the initial configuration settings are implemented, the appliance restarts and the appliance volume wizard appears to let you resize the volume of the web cache.

For more information, refer to the *System configuration* chapter of the *McAfee Web Gateway Product Guide*.

After completing the initial configuration, with or without resizing the web cache, you can log on to the user interface.

## Implement your own initial configuration settings

To implement your own initial configuration settings, follow the instructions of the wizard.

### Task

- 1 In the wizard windows, configure the following:
  - Primary network interface
  - IP address, entered manually or configured dynamically by DHCP



If you plan to configure the explicit proxy mode with High Availability functions (Proxy HA) mode later on, we strongly recommend not to enter a virtual IP address here.

- Network mask (only after entering the IP address manually)
- Default gateway (only after entering the IP address manually)
- Host name
- DNS server (only after entering the IP address manually)

- 2 Review the summary that is displayed after configuring the first settings.
  - If you approve of the summary, confirm and configure the remaining settings:
    - Root password
    - Remote root logon with SSH

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

You can now log on to the user interface.

- If you need to make changes, click **Cancel** and return to step 1.

When the initial configuration settings are implemented, the appliance restarts and the appliance volume wizard appears to let you resize the volume of the web cache.

For more information, refer to the *System configuration* chapter of the *McAfee Web Gateway Product Guide*.

After completing the initial configuration, with or without resizing the web cache, you can log on to the user interface.

---

## Log on to the user interface

To log on to the user interface of Web Gateway, use a browser on your administration system.

### Task

- 1 Open the browser and go to one of the following:

- `http://<IP address>:4711`
- `https://<IP address>:4712`

where `<IP address>` is the IP address from the initial configuration.

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



Google Chrome or Chromium users receive a message stating that Java support by this browser type ends in September 2015. After this date, you cannot access the user interface with this browser type.

A logon window opens.

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

After a successful logon, the setup wizard appears.

---

## Work with the setup wizard

Work with the setup wizard to activate the product and complete the setup procedure.

## Tasks

- [Activate the product on page 19](#)  
To activate the product, review two online documents on licensing and data usage, then import a license and click the activation button.
- [Configure more initial settings on page 20](#)  
Configure initial settings for the time zone, network interfaces, and DNS servers.
- [Solve problems with connecting to the download servers on page 21](#)  
Complete this procedure if the download that is started after activating the product fails due to problems with connecting to the download servers.

## Activate the product

To activate the product, review two online documents on licensing and data usage, then import a license and click the activation button.



You must agree to the content of the online documents if you want to activate the product.

For the licensing procedure, a file with a license key was sent to you. If you have not received it, contact McAfee support. In the meantime, you can use a temporary key.

### Task

- 1 In the **License** section of the setup wizard, click **End User License Agreement** and review the agreement. If you agree to it, select the corresponding checkbox.
- 2 Click **Data Usage Statement** and review the statement. If you agree to it, select the corresponding checkbox.
- 3 Click **Browse** and use the file manager that opens to select the file with the license key, then click **OK**.

The **Activate product** button becomes accessible.

- 4 Click **Activate product**.

Web Gateway is activated and an initial download of files begins to update the information used by the anti-malware and URL filtering modules (engines).

Download progress is indicated by a progress bar at the bottom and explained by a status label.

- 5 Do one of the following:

- Wait until the download finishes successfully, then click **Close wizard**.

This completes the setup procedure. You can now work with the user interface to perform more administration activities.

If you want to configure settings for data collection, configure them and click **Save Changes** when you are done. For more information, refer to the *Data Usage Statement*.



Be sure not to click **Save Changes** to save any other settings before configuring data collection (if you want to do it at all), as data collection starts when this button is clicked for the first time.

For more information on how to work with the user interface, refer to the *McAfee Web Gateway Product Guide*.

- Configure more initial settings.

The download progress remains visible while you continue with the wizard.

If the download fails, an error message appears and the **Network solutions** section becomes accessible in the navigation area. This section allows you to solve problems with connecting to the download servers.

**See also**

*Activate Web Gateway with a temporary license key on page 21*

## Configure more initial settings

Configure initial settings for the time zone, network interfaces, and DNS servers.



You can configure these settings later, working with the user interface. From the **Configuration** top-level menu, select **Date and Time**, **Network Interfaces**, or **Domain Name Service**.

To set administrator passwords, select **Accounts | Administrator Accounts**.

**Task**

- 1 In the **Time zone** section of the wizard, select a time zone for the Web Gateway appliance or leave the default zone (UTC).
- 2 On the **Network interfaces** tab of the **Network settings** section, configure the following:
  - In the **Host name / Fully qualified domain name** field, type a host name for the appliance.
  - In the **Default gateway (IPv4)** or **Default gateway (IPv6)** fields, type an IP address in IPv4 or IPv6 format.  
To configure the default gateway address dynamically, select **Obtain automatically (DHCP)** under **IP settings**.
- 3 On the **Domain name servers** tab of the **Network settings** section, type IP addresses for up to three DNS servers.
- 4 [Optional] In the **Password** section, change the preconfigured administrator password.
- 5 Click **Close wizard**.

The wizard closes and the user interface becomes accessible. A message asks if you want to save the configuration.

- 6 Do one of the following:
  - If you also want to configure settings for data collection, configure them and click **Save Changes** when you are done. For more information, refer to the *Data Usage Statement*.
  - Click **Save Changes** now.

## Solve problems with connecting to the download servers

Complete this procedure if the download that is started after activating the product fails due to problems with connecting to the download servers.

### Task

- 1 In the **Network solutions** section of the wizard, do one of the following, depending on the problem.
  - If the download servers cannot be used for updating filtering information because you are running the appliance in an environment without internet connection, click **Perform offline update** and follow the wizard instructions.
  - If you want to use a next-hop proxy to connect to the download servers, click **Specify next-hop proxy for download** and continue with step 2.
  - If you want to modify the domain name service configuration before connecting to the download servers, click **Specify DNS servers for download** and continue with step 3.
- 2 Under **Next Hop Proxy Definition**, configure the following:
  - a In the **Host** field, type a host name or an IP address for the next-hop proxy in IPv4 or IPv6 format.
  - b In the **Port** field, type a port number for the port on the next-hop proxy that listens to requests from Web Gateway.
  - c In the **User** field, type the user name Web Gateway submits when authenticating to the next-hop proxy.
  - d In the **Password** field, type the password Web Gateway submits when authenticating to the next-hop proxy.
  - e Click **Continue**.

The wizard closes the **Network solutions** section and returns to its main page. If you also want to modify the domain name service configuration, continue with step 3, otherwise continue with step 4.

- 3 Under **Domain Name Server Configuration**, configure the following:
  - a In the **Domain name server** fields, type IP addresses for up to three DNS servers.
  - b Click **Continue**.

The wizard closes the **Network solutions** section and returns to its main page.

- 4 Click **Retry download of engines and patterns**.

The download completes. If the download still does not complete successfully, close the wizard and try to solve the problem otherwise.

---

## Activate Web Gateway with a temporary license key

If you have not yet received a file with a license key from McAfee, you can use a temporary key to activate Web Gateway.

To generate this key, use the activation ID that can be found on a label on your appliance box, for example, *Activation ID: 0923839534*

**Task**

- 1 Use a browser to go to the McAfee Content & Cloud Security Portal at <https://contentsecurity.mcafee.com/>.
- 2 Submit your user name and password.
- 3 On the home page of the portal, type `activate` after the URL mentioned in step 1 and press **Enter**.  
The **Activation** page appears.
- 4 In the **Activation ID** field, type the activation ID from the label on your appliance box, then click **Activate**.
- 5 Follow the online instructions that are provided.

---

## Re-image an appliance

To re-image an appliance, use the appliance software on the CD/DVD or USB drive that is shipped with it.

Instead of using the appliance software on the shipped media for re-imaging, you can download the software for re-imaging from the McAfee Content & Cloud Security Portal and copy it to a USB drive for re-imaging.

The USB drive must be bootable if to be used for re-imaging. You can create a bootable USB drive with a suitable program, for example, Microsoft Win32diskimager.



Re-imaging an appliance overwrites all data that has previously been stored on it.

**Task**

- 1 Back up your appliance configuration on the user interface of Web Gateway, using the functions provided under **Troubleshooting | Backup/Restore**.
- 2 Connect a monitor and keyboard to the appliance.
- 3 Insert the CD/DVD or the USB drive in the appliance.
- 4 Turn on the appliance.
- 5 When prompted, press **F2** to enter the setup menu.
- 6 Select **Boot manager** and then the option for CD/DVD or the USB drive. Then press **Enter**.



On some appliance models, you can press **F6** to enter the boot manager menu directly.

The installation menu appears on the monitor.

- 7 Select an installation mode, then press **Enter**.



Help text is displayed for a selected mode below the menu.

The downloaded software is installed on the appliance. When this installation is completed, the configuration wizard appears.

You can now work with the configuration wizard to implement the initial configuration settings.

## Default serial system console settings

When connecting a serial system console to a Web Gateway appliance for administration purposes, the default settings are as follows.

**Table 2-4 Default serial console settings**

Parameter	Value
Baud rate	19200
Data bits	8
Parity bit	N (no)
Stop bits	1
Short	19200/8-N-1
Flow control	no

## Port assignments on a physical appliance

After setting up a physical appliance, the operating system assigns names to the ports of the network interfaces on the appliance hardware.

The new generation of the appliance hardware includes the following three models:

- WBG-4500-C
- WBG-5000-C
- WBG-5500-C

There are also several older models:

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

The model number is located on a label on top of the hardware chassis.

The diagrams in the following sections show the port assignments for each appliance model.

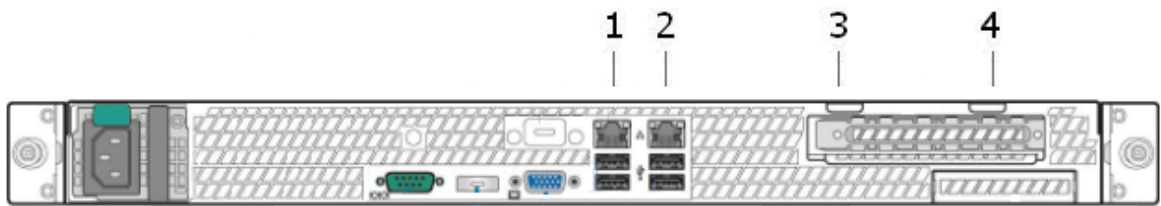
### Port assignments on the new generation appliance models

The following diagrams show the port assignments for the new generation appliance models.

#### WBG-4500-C

This appliance model has two network interfaces in the middle of its rear panel (NIC 1 and NIC 2).

A dual port card with two more network interfaces (NIC 3 and NIC 4) is accessible through the card slot on the right.

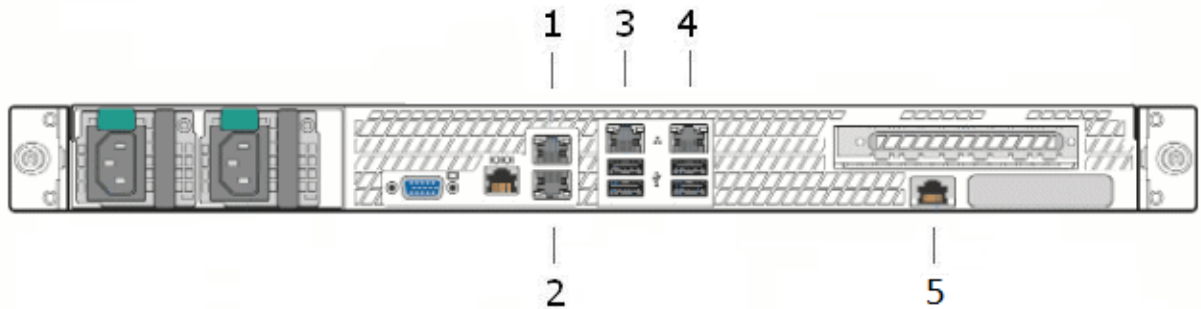


Ports and names for these interfaces:

Position	Network interface port	Name assigned by the operating system
1	NIC 1 (onboard)	eth0
2	NIC 2 (onboard)	eth1
3	NIC 3 (leftmost on dual port card)	eth3
4	NIC 4 (rightmost on dual port card)	eth2

### WBG-5000-C

This appliance model has four network interfaces (NIC 1–4) in the middle of its rear panel and an RMM network interface on the right.



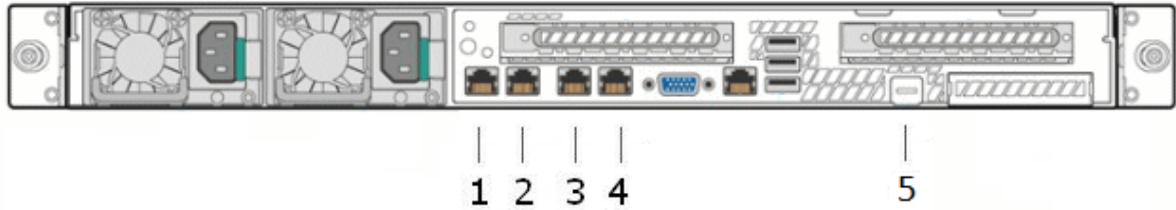
Ports and names for these interfaces:

Position	Network interface port	Name assigned by the operating system
1	NIC 1	eth0
2	NIC 2	eth1
3	NIC 3	eth2
4	NIC 4	eth3
5	RMM For operating the RMM (Remote Management Module) and BMC (Baseboard Management Controller)	



### WBG-5500-C

This appliance model has four network interfaces (NIC 1–4) in the middle of its rear panel and an RMM network interface on the right.



Ports and names for these interfaces:

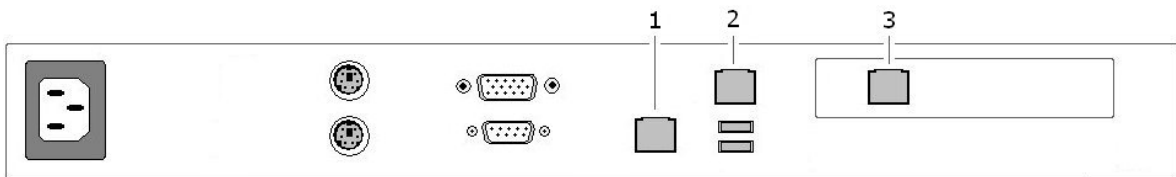
Position	Network interface port	Name assigned by the operating system
1	NIC 1	eth0
2	NIC 2	eth1
3	NIC 3	eth2
4	NIC 4	eth3
5	RMM For operating the RMM (Remote Management Module) and BMC (Baseboard Management Controller)	

### Port assignments on the older appliance models

The following diagrams show the port assignments for the older appliance models.

#### WBG-4000-B

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



Ports and names for these interfaces:

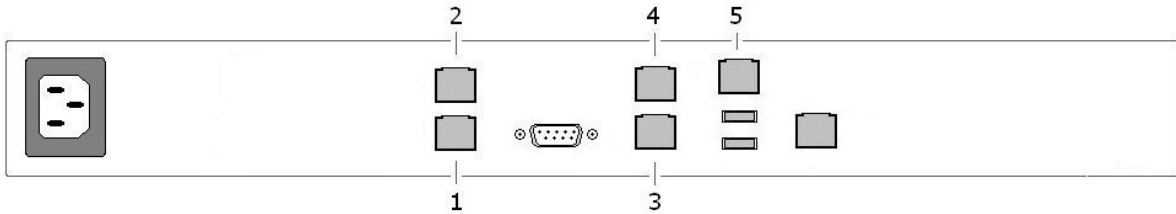
Position	Network interface with port	Interface name of the operating system
1	e1000e	eth0
2	e1000	eth1
3	e1000e	eth2



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

### WBG-4500-B

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

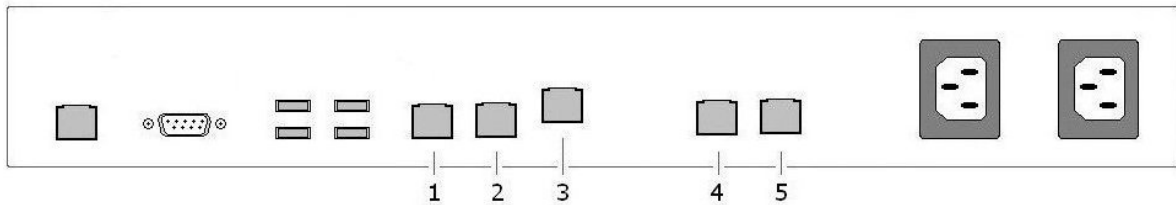


Ports and names for these interfaces:

Position	Network interface with port	Interface name of the operating system
1	igb	eth0
2	igb	eth1
3	igb	eth2
4	igb	eth3
5	e1000e	eth4

### WBG-5000-B

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

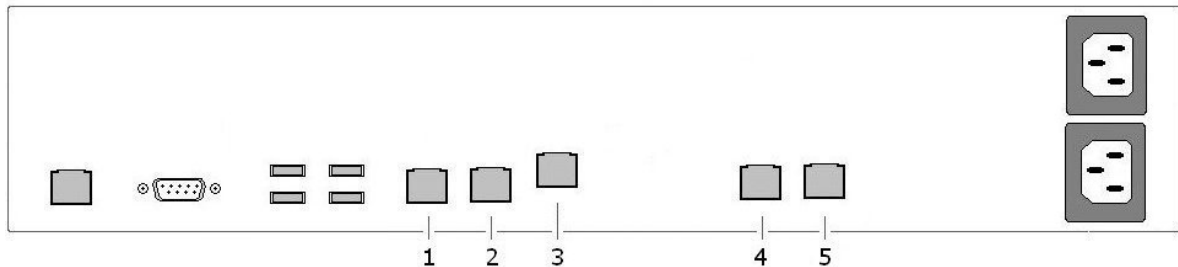


Ports and names for these interfaces:

Position	Network interface with port	Interface name of the operating system
1	igb	eth0
2	igb	eth1
3	rmm and bmc For operation of the RMM (Remote Management Module) and BMC (Baseboard Management Controller)	
4	e1000e	eth3
5	e1000e	eth2

## WBG-5500-B

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



Ports and names for these interfaces:

Position	Network interface with port	Interface name of the operating system
1	igb	eth0
2	igb	eth1
3	rmm and bmc For operation of the RMM (Remote Management Module) and BMC (Baseboard Management Controller)	
4	e1000e	eth3
5	e1000e	eth2

## Memory upgrade

When running Web Gateway on an older appliance model (A, B, or E in the model short code), make sure that sufficient memory (RAM) size is available. We recommend a size of at least 8 GB. You can install additional memory modules to upgrade.

The appliances of the model C series already meet the current memory recommendations.

When upgrading memory on any appliance model, it is important that you only install the appropriate modules for Intel-based or Dell-based appliances, depending on what model you are using.



Memory upgrades that follow McAfee recommendations do not void the hardware warranty.

### Memory modules for Intel-based appliances

The following table shows the memory recommendations for appliances of the model B series that are Intel-based. Purchase these memory modules from your usual vendor.

**Table 2-5** Memory recommendations

Appliance model	Intel server model	Recommended memory size	Recommended memory model	Recommended memory configuration
WBG-4000-B	SR1530SH	8	ATP AJ56K72H8BJE6S	4 x 2 GB ATP modules
WBG-4500-B	SR1630GPRX	8	ATP AQ56M72D8BKH9M 2 GB modules	4 x 2 GB ATP modules

**Table 2-5 Memory recommendations** (continued)

Appliance model	Intel server model	Recommended memory size	Recommended memory model	Recommended memory configuration
WBG-5000-B	SR1625URSAS	24	Kingston KVR16R11S8/4I	6 x 4 GB modules (2-2-2 population)
WBG-5500-B	SR2625URLXRNA	24	Kingston KVR16R11S8/4I	6 x 4 GB modules (1-1-1/1-1-1 population)



For the latest updates of these recommendations, see this article at the McAfee Knowledge Center: [KB82852](#).

### Memory modules for Dell-based appliances

Memory modules for Dell-based appliances can be obtained from the online store at the Dell website. This website also provides information on how to install the modules.

We recommend a memory upgrade for the following Web Gateway (Dell) appliance models:

- WW1100E (Dell PowerEdge R200)
- WW1900E (Dell PowerEdge 1950)
- WW2900E (Dell PowerEdge 2950)
- WBG-5000-A (Dell PowerEdge R610)
- WBG-5500-A (Dell PowerEdge R710)

### Purchase Dell memory modules

You can purchase memory modules for a Dell-based appliance model from the online store at the Dell website.



The Dell website is subject to change and has a different look in different countries. The following procedure applies to the current US website.

#### Task

- 1 Go to the Dell website at <http://www.dell.com>.
- 2 From the top-level menu bar on the home page, select **For Work | Servers, Storage & Networking**.
- 3 Under **Other Ways to Shop**, select **Parts for Your Dell | Parts for Your Enterprise System | PowerEdge Servers**.
- 4 From the list of servers, select the model that you want to purchase memory modules for, for example, **PowerEdge 1950** (= WW1900E).
- 5 On the server page, expand **Memory Upgrades for Your <server name>** and review the modules that are offered.
- 6 Complete the purchasing procedure in the usual way.

### Get information on how to install memory modules

You can view or download instructions for installing memory modules on an appliance at the Intel and Dell websites.



The websites are subject to change and have different looks in different countries. The following procedures apply to the current US websites.

## Get installation information for Intel memory modules

Review information on how to install a memory module in the service manual for an Intel server system.


### Task

- 1 Go to the Intel website at <http://www.intel.com>.
- 2 From the menu on the welcome page, select **Support | Support Home**.
- 3 Under **Find support topics by product**, select the following, then click **Find**.
  - Product family: **Server Products**
  - Product line: **Intel Server Systems**
  - Product name: a server name, for example, **Intel Server System SR1630GP**

In the list of product names, selecting a name with a particular product code sometimes also gives you access to information about products with an *extended* code name.



For example, selecting **Intel Server System SR1630GP**, together with **Documents & Guides** (see under *d*), gives you access to the manuals for *Intel Server System SR1630GP* and *Intel Server System SR1630GPRX (= WBG-4500-B)*.

- Support information: **Documents & Guides**
- 4 Under **Documents & Guides**, select the service guide.
    -  For *Intel Server System SR1530SH*, the relevant manual is the user's guide.
  - 5 Open the document PDF and review the information in the *Installing and Removing Memory* section of the *Hardware Installations and Upgrades* chapter.

## Get installation information for Dell memory modules

Review information on how to install a memory module in the hardware manual for a Dell server system.

### Task

- 1 Go to the Dell website at <http://www.dell.com>.
- 2 From the top-level menu bar on the home page, select **Support | Support by Product**.

If the product page that appears is about your appliance model, continue with step 3, otherwise complete the following substeps to navigate to your model.

  - a Below the current product name, click **View a different product**.
  - b Under **Browse for your product**, click **View products**, and select **Servers, Storage & Networking | PowerEdge**.
  - c Select a model from the list of servers, for example, **PowerEdge R610 (= WBG-5000-A)**.
- 3 On the product page, click **Manuals**, then open the PDF with the *Hardware Owner's Manual*.
- 4 Review the information in the *System Memory* section of the *Installing System Components* chapter.



# 3

## Installing a PCI card

PCI (Peripheral Component Interconnect) cards can be installed on a Web Gateway appliance, for example, to provide fiber connectivity or to enable the use of a Hardware Security Module (HSM).

### Contents

- ▶ *Supported fiber NICs*
- ▶ *Supported copper NICs*
- ▶ *Supported HSM cards*
- ▶ *Install a PCI card*

## Supported fiber NICs

Fiber network interface cards (fiber NICs) are PCI cards that provide fiber connectivity. To provide fiber connectivity on a Web Gateway appliance, you must purchase a fiber NIC from an appropriate vendor and install it.

Supported fiber NICs include a 1GbE and a 10GbE version. If you want to work with a 10GbE fiber NIC, you must install a transceiver, known as *gbic*, which you must also purchase from a vendor.



McAfee only supports the fiber NICs and transceivers in this guide. Installing supported fiber NICs does not void the hardware warranty.

The following cards can be installed.

**Table 3-1 Supported 1GbE and 10GbE fiber card types**

Vendor	Type	Subtype	Medium	Ports	Height
Intel	i340-F4	E1G44HT	1000BASE-SX	4	Full
HotLava	Tambora 64G4	4ST2830A2	10GBASE-SR Required transceiver (gbic): HLSR10G3A SFP+ HotLava modules/optics	4	Low with full profile bracket mounted
HotLava	Tambora 80G4S-G3	4ST3830A1F	10GBASE-SR Required transceiver (gbic): HLSR10G4A SFP+ HotLava modules/optics	4	Low with full profile bracket mounted

The cards can be installed on the following Web Gateway appliance models.

**Table 3-2 Suitable Web Gateway appliance models**

Model	Height units	Slots
WBG-5000-B	1	1 x PCI full height
WBG-5000-C	1	1 x PCI full height

**Table 3-2 Suitable Web Gateway appliance models** (continued)

Model	Height units	Slots
WBG-5500-B	2	2 x PCI low profile 3 x PCI full height
WBG-5500-C	1	2 x PCI full height



The WBG-5000-B and WBG-5000-C models have only one slot for a PCI card. The WBG-5500-B and WBG-5500-C models have two, which allows you to install an HSM card and a fiber card.

Configurations with more than one fiber card on an appliance have not been validated by McAfee.

## 1GbE fiber NIC

The supported card type for a 1GbE fiber NIC on a Web Gateway appliance is *Intel i340-F4*.

This fiber card comes equipped with 4 fixed optics, supporting 1000BASE-SX media with LC connectors. It is a full-height PCIe card.

The following table shows how the ports for the interfaces on the onboard network interface card and the fiber card are mapped to the interface names used by the operating system.

**Table 3-3 Port mapping with 1GbE fiber card installed**

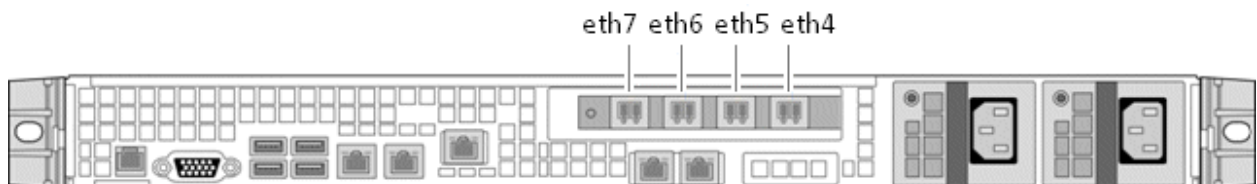
Port on onboard or fiber NIC	Interface name of the operating system
Onboard NIC port 1	eth0
Onboard NIC port 2	eth1
Onboard NIC port 3	eth2
Onboard NIC port 4	eth3
1GbE fiber NIC port 1 (rightmost)	eth4
1GbE fiber NIC port 2	eth5
1GbE fiber NIC port 3	eth6
1GbE fiber NIC port 4 (leftmost)	eth7

The mapping table shows that the ports on the fiber card and, consequently, the interface names are numbered in reverse order, compared to their locations on the rear of an appliance.

From left to right, the order is as follows.

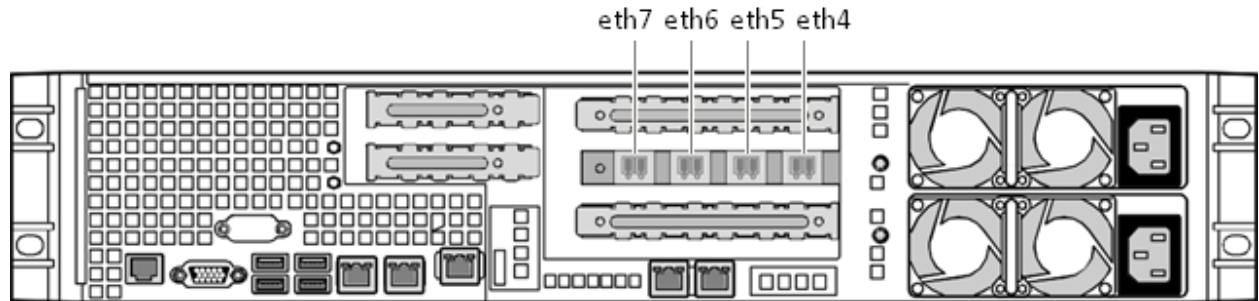
```
eth7 - eth6 - eth5 - eth4
```

For example, on the rear of the WBG-5000-B appliance model, the order is as shown in the following diagram.

**Figure 3-1 Interface names for 1GbE fiber card ports on WBG-5000-B**

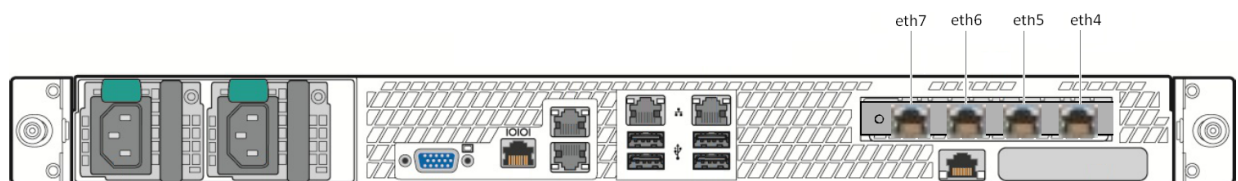


On the rear of WBG-5500-B, the order is as shown.



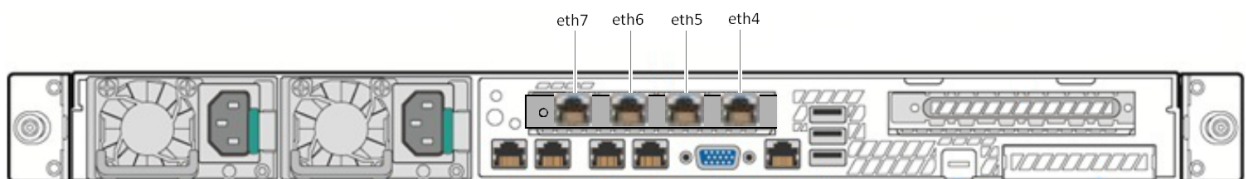
**Figure 3-2 Interface names for 1GbE fiber card ports on WBG-5500-B**

On the rear of WBG-5000-C, the order is as shown.



**Figure 3-3 Interface names for 1GbE fiber card ports on rear of WBG-5000-C**

On the rear of WBG-5500-C, the order is as shown.



**Figure 3-4 Interface names for 1GbE fiber card ports on rear of WBG-5500-C**



The WBG-5500-C appliance model has two slots for inserting a PCI card. Insert the fiber card in the slot shown as occupied in the diagram.

## 10GbE fiber NIC

The supported card types for a 10GbE fiber network interface card on a Web Gateway appliance are *HotLava Tambora 64G4* and *HotLava Tambora 80G4S-G3*.

These cards are low profile PCIe cards, each with a full height bracket mounted by default to accommodate the bracket height of the Web Gateway appliance models.

If you want to use a fiber card of this type, you must also purchase and install a transceiver with gbic components as follows: 4 HotLava HLSR10G3A SFP+ modules/optics for 10GBASE-SR media with LC connectors.

The following table shows how the ports for the interfaces on the onboard network interface card and the fiber card are mapped to the interface names used by the operating system.

**Table 3-4 Port mapping with 10GbE fiber card installed**

Port on onboard or fiber NIC	Interface name of the operating system
Onboard NIC port 1	eth0
Onboard NIC port 2	eth1

**Table 3-4 Port mapping with 10GbE fiber card installed** *(continued)*

Port on onboard or fiber NIC	Interface name of the operating system
Onboard NIC port 3	eth2
Onboard NIC port 4	eth3
10GbE fiber NIC port1 (leftmost)	eth4
10GbE fiber NIC port2	eth5
10GbE fiber NIC port3	eth6
10GbE fiber NIC port4 (rightmost)	eth7

The mapping table shows that the ports on the fiber card and, consequently, their interface names are numbered in normal order, compared to their locations on the rear of an appliance.

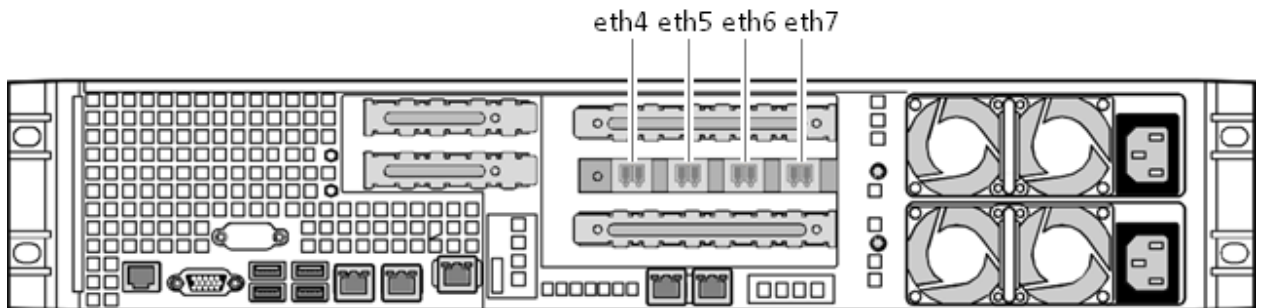
From left to right, the order is as follows.

```
eth4 - eth5 - eth6 - eth7
```

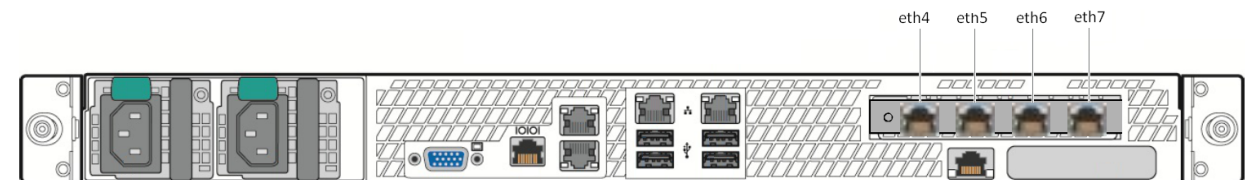
For example, on the rear of the WBG-5000-B appliance model, the order is as shown in the following diagram.

**Figure 3-5 Interface names for 10GbE fiber card ports on rear of WBG-5000-B**

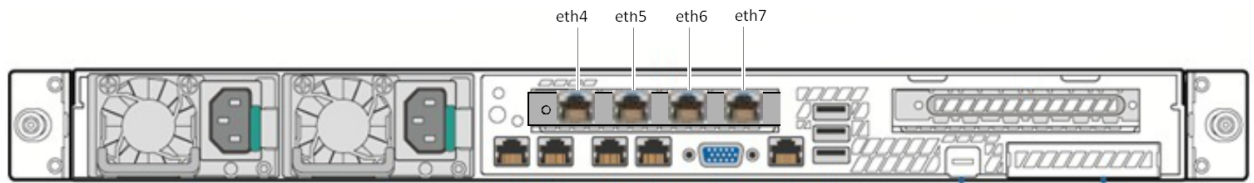
On the rear of WBG-5500-B, the order is as shown.

**Figure 3-6 Interface names for 10GbE fiber card ports on rear of WBG-5500-B**

On the rear of WBG-5000-C, the order is as shown.

**Figure 3-7 Interface names for 10GbE fiber card ports on rear of WBG-5000-C**

On the rear of WBG-5500-C, the order is as shown.



**Figure 3-8 Interface names for 10GbE fiber card ports on rear of WBG-5500-C**



The WBG-5500-C appliance model has two slots for inserting a PCI card. Insert the fiber card in the slot shown as occupied in the diagram.

## Supported copper NICs

Copper network interface cards (copper NICs) are PCI cards for connections that use copper cables. On a Web Gateway appliance, you can run a quad port copper NIC with a bandwidth of 1GbE.

If you want to run a copper NIC on a Web Gateway appliance, purchase it from an appropriate vendor and install it.



McAfee only supports the copper NICs described in this guide. Installing supported copper NICs does not void the hardware warranty.


The following card can be installed.

**Table 3-5 Supported copper NIC card type**

Vendor	Type	Subtype	Medium	Ports	Height
Intel	i350-T4v2	i350T4V2BLK	Copper	4	Low with full profile bracket mounted

The card can be installed on the following Web Gateway appliance models.

**Table 3-6 Suitable Web Gateway appliance models**

Model	Height units	Slots
WBG-4500-C	1	1 x PCI full height
 On this appliance model, you must remove the pre-installed dual port card before installing the copper card, as only one additional NIC is supported here.		
WBG-5000-C	1	1 x PCI full height
WBG-5500-C	1	2 x PCI full height

## 1GbE copper NIC

The supported card type for a 1GbE copper NIC on a Web Gateway appliance is *Intel i350-T4v2*.

The ports on the copper card and, consequently, their interface names are numbered in reverse order, compared to their locations on the rear of an appliance.

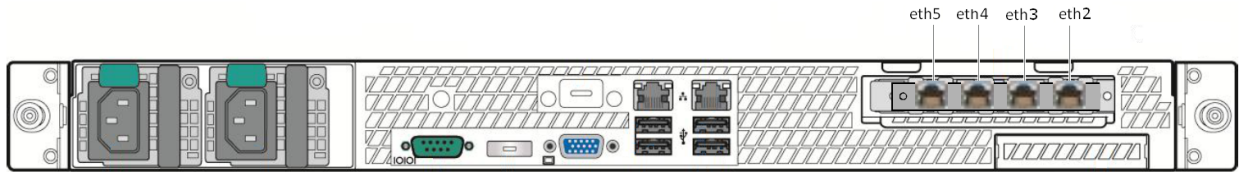
When a copper card is installed on the WBG-4500-C appliance model, the pre-installed onboard dual port card must first be removed. The model is left with only two onboard network interfaces then, so the numbering and order of the additional interface names is, from left to right, as follows.

```
eth5 - eth4 - eth3 - eth2
```

On the other models, the order is as follows.

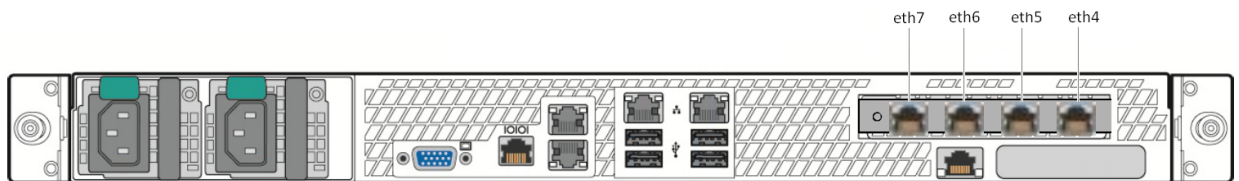
```
eth7 - eth6 - eth5 - eth4
```

The following diagram shows the position of the interfaces provided by a copper card and their names on the rear of the WBG-4500-C appliance model



**Figure 3-9 Interfaces for 1GbE copper card ports on WBG-4500-C**

On the rear of the WBG-5000-C appliance model, the positions of these interfaces are as follows.



**Figure 3-10 Interfaces for 1GbE copper card ports on WBG-5000-C**

For diagrams with the interface positions on the other models, see the *1GbE fiber NIC* section.

## Supported HSM cards

A Hardware Security Module is made available on a PCI card that is known as *HSM card*. To use the functions of this module on a Web Gateway appliance, you must purchase an HSM card from an appropriate vendor and install it.



McAfee only supports the HSM cards in this guide. Installing supported HSM cards does not void the hardware warranty.

The following cards can be installed.

**Table 3-7 Supported HSM card type**

Vendor	Type	Subtype	Height
Thales	nShield nCipher	500e F3	Full
Thales	nShield Solo 6000+		Full

For more information on working with a Hardware Security Module, see the *Web filtering* chapter of the *McAfee Web Gateway Product Guide*.

## Install a PCI card

To install a PCI card on a Web Gateway appliance, unplug the appliance, remove its cover, and insert the card in a suitable slot.



To avoid damage to the appliance or the PCI card caused by electrostatic discharge (ESD), make sure that you work in an ESD-protected area.



Some appliance models secure the PCI card with a screw, for example, WBG-5000-B, others use retention clips, for example, WBG-5500-B.

### Task

1 Turn off the appliance and unplug the power cord.

2 Remove the appliance cover.



Turn off and unplug the appliance *before* removing its cover. Failure to do so could endanger you and damage the appliance or the PCI card.

3 Insert the PCI card.

a Remove the PCI riser assembly.

b If retention clips are used, open the front and rear clips on the assembly.

c Choose a slot on the riser card of the assembly for inserting the PCI card and remove the filler panel from this slot.



On model WBG-5500-C, you must use riser slot 2.

d If a securing screw is used, remove it.

e Push the PCI card into the slot until it seats in the riser card connector.



Use caution when pushing the PCI card, as excessive force can break the connector.

f Secure the PCI card with the screw or close the front and rear retention clips.

g Re-install the assembly.

4 Re-attach the appliance cover and plug in the power cord.

5 Turn on the appliance.

For more information on the installation procedure, refer to the *Intel Server System SR1625UR Service Guide (WBG-5000-B)* or *Intel Server System SR2600UR/SR2625UR Service Guide (WBG-5500-B)*.

You can download these documents from the Intel website under:

- [http://download.intel.com/support/motherboards/server/s5520ur/sb/e52881005\\_sr1625ur\\_sg1.pdf](http://download.intel.com/support/motherboards/server/s5520ur/sb/e52881005_sr1625ur_sg1.pdf) – WBG-5000-B
- [http://download.intel.com/support/motherboards/server/s5520ur/sb/E51243-007\\_SR2600UR\\_SR2625UR\\_SG.pdf](http://download.intel.com/support/motherboards/server/s5520ur/sb/E51243-007_SR2600UR_SR2625UR_SG.pdf) – WBG-5500-B



# 4

## Installing hardware administration tools

When running Web Gateway on a physical appliance, you can use tools to perform hardware-related administration jobs. You can install these tools after setting up Web Gateway.

### Contents

- ▶ *Tools for administering the Web Gateway hardware*
- ▶ *Install the Platform Confidence Test tool*
- ▶ *Run a hardware test with the Platform Confidence Test tool*
- ▶ *Configure the Remote Management Module*
- ▶ *Install the Active System Console*
- ▶ *Enable the SNMP Subagent*

---

## Tools for administering the Web Gateway hardware

Several tools are available for administering the hardware of a Web Gateway appliance.

### Platform Confidence Test tool

The Platform Confidence Test (PCT) tool allows you to test the hardware functions of an appliance. When performing a test, the appliance must not be connected to other network devices.

The test results are stored in the *result.log* file, which you can copy to a USB drive for further use.

### Remote Management Module

The Remote Management Module (RMM) enables you to administer the hardware functions of an appliance remotely.

Together with this tool, another tool is installed in the same procedure. This tool is the Baseboard Management Controller (BMC). It must also be running if you want to use the Active System Console for retrieving debugging information.

The interface for the Remote Management Module and the Baseboard Management Controller are on the rear panel of an appliance box.

### Active System Console

The Active System Console (ASC) is a web-based debugging tool. It provides information on hardware errors involving chassis, storage, fans, processors, memory, power supplies, and other components.



We recommend that, rather than using the Active System Console to retrieve debugging information for your hardware, you work with the Remote Management Module to obtain this information.

Errors are detected by the Baseboard Management Controller which is installed together with the Remote Management Module. The Baseboard Management Controller accesses system event and sensor data recordings on an appliance.

The Active System Console allows you to configure settings for the Baseboard Management Controller, for example, its IP address.

The tool also enables you to send hardware-related data to McAfee.

### SNMP Subagent

When SNMP (Simple Network Management Protocol) monitoring is configured on an appliance, you can use the SNMP Subagent (SNMPSA) to retrieve hardware-related information, for example, CPU status, status of power supplies, or current sensor values.

SNMP information on the status of hardware components is stored in the Management Information Base (MIB).

To provide the information, the database uses a tree structure of objects, which are related to particular hardware components and other items. Objects are identified and accessed using object IDs (OIDs).

---

## Install the Platform Confidence Test tool

Install the Platform Confidence Test (PCT) tool to retrieve information on hardware errors. For each appliance model, there is a particular version of the tool.

### Task

- 1 Download the appropriate tool version from the McAfee Content & Cloud Security Portal. Tool versions are available in zipped format.
- 2 Extract the content of a downloaded .zip file into the root directory of a USB drive that is formatted in Microsoft DOS mode.
- 3 Attach the USB drive to the appliance.
- 4 Restart the appliance.
- 5 When prompted, press **F2** to enter the setup menu.
- 6 Select **Server Management | Console Redirection** and make sure **Console Redirection** is disabled.
- 7 Select **Boot Manager** and click **EFI Shell**.

The appliance is restarted in EFI (Extensible Firmware Interface) shell mode.

The EFI shell mode runs the *startup.nsh* procedure from the USB drive and displays a diagnostics menu.

You can terminate the diagnostic cycle by pressing **F10**.

---

## Run a hardware test with the Platform Confidence Test tool

To test the appliance hardware, run the Platform Confidence Test (PCT) tool and save the resulting information in a log file.

### Before you begin

Make sure the appliance is not connected to any other network component.



**Task**

- 1 From the diagnostics menu of the tool, select a test type.



When testing the network interface ports, you can connect any port to any other port in the same system using a cross-over cable.

The test is executed and the result written into a log file on a RAM disk. The name of the log file is *result.log*.

- 2 Copy the *result.log* file to the USB drive.
  - a Run the *map* command.
  - b Identify the USB drive in the list that appears. Then enter the following command:

```
cp result.log blk0: <name of the USB drive>
```

In this command, *blk0* is a device parameter that is required when using a USB drive.



Different device parameters can be specified here in some cases.

We recommend that after performing the comprehensive or comprehensive looping test, you do a full AC power cycle (by removing power from the system) before you continue after the test.

This resets all controllers and ensures that they are running in an expected mode.

---

## Configure the Remote Management Module

Configure the Remote Management Module (RMM) to administer the appliance hardware remotely. Together with this tool, the Baseboard Management Controller (BMC) can be installed in the same procedure to support the Remote Management Module.

**Task**

- 1 Connect the interfaces for the Remote Management Module or the Baseboard Management Controller or for both on the rear panel of the appliance box to the network.
- 2 Restart the appliance.
- 3 During the start phase, press **F2**.

A configuration menu appears.
- 4 Select **Server Management | BMC LAN Configuration**.
- 5 Under **Baseboard LAN configuration**, configure an IP address, a subnet mask, and a gateway IP address.
- 6 Under **Intel (R) RMM3 LAN configuration** (for WBG-xxxx-B models) or **Intel (R) RMM4 LAN configuration** (for WBG-xxxx-C models), configure an IP address, a subnet mask, and a gateway IP address.
- 7 Under **User configuration**, configure a user name and password to allow an initial user to access the Remote Management Module.
- 8 Press **F10**, and in the dialog window that appears, click **Yes** to save your settings.

The Remote Management Module is now available for administering the appliance hardware remotely. You can access the module using the IP address that you have configured.

The interface for the Remote Management Module and the Baseboard Management Controller is located between the network interfaces on the rear panel of an appliance box. For a diagram that shows the location of the interfaces, see the *Port assignments* section in the *Setting up Web Gateway* chapter of this guide.

---

## Install the Active System Console

Install the Active System Console (ASC) to retrieve debugging information about the appliance hardware.



We recommend that, rather than using the Active System Console to retrieve debugging information for your hardware, you work with the Remote Management Module to obtain this information.

### Task

- 1 Log on to the appliance from a system console, using SSH.run the following command:

```
asc-enable
```

- 2 Run the following command

```
asc-enable
```

- 3 When prompted, create an administrator password.

If a message on strong password setting is displayed, respond according to your requirements.

After the password has been set, the Active System Console is started.

- 4 Use a web browser to access the ASC user interface under:

```
https://<IP address of the monitored appliance>:9393
```

When you start the appliance next time, the Active System Console is automatically started with it.

You can disable the Active System Console, using the *asc-disable* command.

For more information, see the help information on the user interface of the Active System Console and the documentation that is provided with the hardware.

---

## Enable the SNMP Subagent

Enable the SNMP Subagent (SNMP\_SA) from a system console to retrieve information on the hardware status of an appliance.

### Task

- 1 Make sure you have configured the SNMP settings on the user interface of the appliance.

For information on how to configure these settings, refer to the *Monitoring* chapter of the *McAfee Web Gateway Product Guide*

- 2 From a system console, log on to the appliance, using SSH.

- 3 Run the following command:

```
snmpsa-enable
```

The SNMP Subagent is enabled.

You can disable the SNMP Subagent using the *snmpsa-disable* command.

When the SNMP Subagent is enabled, hardware status information is available under the SNMP protocol.

An overview of the available information is provided in MIB (Management Information Base) files, which are located in the file system of the monitored appliance. The path to these files is `/usr/local/snmpsa/mibs`.

For more information on working with the SNMP Subagent, refer to the *Intel SNMP Subagent User Guide*.

You can download this document from the Intel website under <http://www.intel.com/support/motherboards/server/sysmgmt/sb/CS-029304.htm>.



# 5

## Installing Web Gateway on a blade server

You can use a blade server in a blade system enclosure as the hardware platform for Web Gateway.

### Contents

- ▶ *Supported blade servers and enclosures*
- ▶ *Installing the blade server system*
- ▶ *Network setup for Web Gateway on a blade server*
- ▶ *Port assignments on a blade server*

---

## Supported blade servers and enclosures

A blade server is a modular server that is installed in a blade system enclosure.



The blade server models that are provided for use with Web Gateway are also known as *McAfee Blades*.

Web Gateway can run on the following blade server models:

- ProLiant BL460c G6
- ProLiant BL460c G6.5
- ProLiant BL460C G8

The blade servers can be installed in the following enclosure models:

- M3 (c3000)
- M7 (c7000)

---

## Installing the blade server system

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

A blade system enclosure that has blade servers installed is referred to as a *blade server system*.

For a detailed description of how to install a blade server system, refer to the documentation of the McAfee partner (Hewlett-Packard) who provides blade servers for Web Gateway. The documentation is available on their website.

## Preparing the installation of the blade server system

Several requirements must be met for installation of a blade server system.

When preparing the installation, the following is important to consider.

### Environment of the blade server system

You need to consider the environment of the blade server system.

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

### Completeness of shipment

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

- Blade server enclosure (M3 or M7) with blade servers
- Power cords
- Network cables

### IP addresses for the blade server system

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

- Onboard Administrator
- Integrated Lights Out (iLO) modules — 8 to 16 addresses (depending on your configuration)
- Interconnect modules — 4 addresses
- Blade servers (number of addresses depending on your configuration)

For more detailed information, refer to the *Site Planning Guide* and the *Setup and Installation Guide* that is provided for each enclosure model on the website of the McAfee partner.

## Install the blade server system

To install the blade server system, install the blade system enclosure, insert the interconnect modules in the enclosure, and turn on the enclosure.

### Tasks

- [Install the blade system enclosure on page 47](#)  
To install the blade system enclosure, unpack it, install components, and connect a monitor and keyboard.
- [Install the interconnect modules on page 47](#)  
To install the interconnect modules, inserted them in the interconnect bays on the blade system enclosure.
- [Turn on the blade system enclosure on page 48](#)  
Supply power to the blade system enclosure and turn it on.
- [Install Web Gateway on a blade server on page 48](#)  
To install Web Gateway on a blade server, download the appliance software, choose an installation device and a blade server, and perform the installation procedure.

## Install the blade system enclosure

To install the blade system enclosure, unpack it, install components, and connect a monitor and keyboard.

### Task

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



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

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



We recommend that you install all power supplies and fans that were shipped with the enclosure to ensure redundancy in case one of these components fails.

- 5 Install the Onboard Administrator and the Integrated Lights Out System.
- 6 Connect a monitor and keyboard to the enclosure.
- 7 Attach power cords to the monitor and the enclosure, but do not yet connect the power supplies.

For more information, refer to the *Setup and Installation Guide*, the *Onboard Administrator User Guide*, and the *Integrated Lights-Out User Guide* that are provided for each enclosure model on the website of the McAfee partner.

## Install the interconnect modules

To install the interconnect modules, insert them in the interconnect bays on the blade system enclosure.

The Onboard Administrator lets you view diagrams of the enclosure. Using the mouse-over function, you can locate the position of the interconnect bays on the rear side of the enclosure.

The M3 enclosure model has four interconnect bays, the M7 model has eight. These modules are either pass-through modules or switches.

### Task

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

## Turn on the blade system enclosure

Supply power to the blade system enclosure and turn it on.

### Task

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



We recommend that you use two power circuits to ensure all blade servers in the enclosure turn on.

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

- 2 Turn on the blade system enclosure.

You can now install the Web Gateway appliance software on a blade server in the enclosure.

## Install Web Gateway on a blade server

To install Web Gateway on a blade server, download the appliance software, choose an installation device and a blade server, and perform the installation procedure.

You can download the Web Gateway appliance software in ISO or USB format from the McAfee Content & Cloud Security Portal under [https://contentsecurity.mcafee.com/software\\_mwg7\\_download](https://contentsecurity.mcafee.com/software_mwg7_download)

Different devices can be used to install Web Gateway on a blade server, depending on the enclosure model:

- Internal CD/DVD drive — M3
- External CD/DVD drive — M7
- USB drive — M3 and M7
- Virtual media — M3 and M7

After choosing an installation device, you need to complete one of the following tasks.

### Tasks

- *Use the internal CD/DVD drive to install Web Gateway on a blade server on page 49*  
If your enclosure model is M3, you can use the internal CD/DVD drive to install the Web Gateway appliance software on a blade server in the enclosure.
- *Use an external CD/DVD drive to install Web Gateway on a blade server on page 49*  
If your enclosure model is M7, you can use an external CD/DVD drive to install the Web Gateway appliance software on a blade server in the enclosure.
- *Use a USB drive to install Web Gateway on a blade server on page 50*  
You can use a USB drive to install the Web Gateway appliance software on a blade server in either of the two enclosure models.
- *Use virtual media to install Web Gateway on a blade server on page 50*  
You can use virtual media to install the Web Gateway appliance software on a blade server in either of the two enclosure models. The blade system enclosure provides an option for a virtual installation of McAfee Web Gateway on a server in the enclosure using an ISO image that is stored on one of your local drives.



### Use the internal CD/DVD drive to install Web Gateway on a blade server

If your enclosure model is M3, you can use the internal CD/DVD drive to install the Web Gateway appliance software on a blade server in the enclosure.

#### Task

- 1 Insert a CD or DVD with the Web Gateway appliance software on it in the internal CD/DVD drive of the enclosure.
- 2 Open the Onboard Administrator of the enclosure and select a blade server to install Web Gateway on.
- 3 Click the **Virtual Devices** tab.
- 4 Use this tab to connect the internal CD/DVD drive to the blade server.
- 5 Click the **Boot Options** tab and set **One Time Boot from** to **CD-ROM**.
- 6 Turn on the blade server.
- 7 Follow the instructions for installing Web Gateway that appear on the monitor you connected to the enclosure.

When the installation is completed, you can log on to the user interface of Web Gateway.

For information about logging on and how to continue, see the *Setting up Web Gateway* chapter in this guide.

### Use an external CD/DVD drive to install Web Gateway on a blade server

If your enclosure model is M7, you can use an external CD/DVD drive to install the Web Gateway appliance software on a blade server in the enclosure.

#### Task

- 1 Insert a CD or DVD with the Web Gateway appliance software on it in the external CD/DVD drive.
- 2 Use the USB SUV cable that is shipped with the enclosure to connect the drive to the blade server you want to install Web Gateway on.
- 3 Open the Onboard Administrator of the enclosure and select the blade server.
- 4 Click the **Boot Options** tab and set **One Time Boot from** to **CD-ROM**.
- 5 Turn on the blade server.
- 6 Follow the instructions for installing Web Gateway that appear on the monitor you connected to the enclosure.

When the installation is completed, you can log on to the user interface of Web Gateway.

For more information about logging on and how to continue, see the *Setting up Web Gateway* chapter in this guide.

### Use a USB drive to install Web Gateway on a blade server

You can use a USB drive to install the Web Gateway appliance software on a blade server in either of the two enclosure models.

#### Task

- 1 Use the USB SUV cable that is shipped with the enclosure to connect the USB drive to the blade server you want to install Web Gateway on.
- 2 Open the Onboard Administrator of the enclosure and select the blade server.
- 3 Click the **Virtual Devices** tab.
- 4 Click the **Boot Options** tab and set **One Time Boot from** to **USB**.
- 5 Turn on the blade server.
- 6 Follow the instructions for installing Web Gateway that appear on the monitor you connected to the enclosure.

When the installation is completed, you can log on to the user interface of Web Gateway.

For information about logging on and how to continue, see the *Setting up Web Gateway* chapter in this guide.

### Use virtual media to install Web Gateway on a blade server

You can use virtual media to install the Web Gateway appliance software on a blade server in either of the two enclosure models. The blade system enclosure provides an option for a virtual installation of McAfee Web Gateway on a server in the enclosure using an ISO image that is stored on one of your local drives.

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

#### Task

- 1 Open the Onboard Administrator of the enclosure and select a blade server to install Web Gateway on.
- 2 Click **iLO**, then click **Web Administration**.  
  
A new browser window opens providing access to the iLO (integrated Lights-Out) web user interface.
- 3 Click the **Virtual Media** tab, then click **Virtual Media**.  
  
The **Virtual Media** window opens.
- 4 Choose the **Virtual Floppy/USB Key** or **Virtual CD/DVD-ROM** section of the window for installing Web Gateway and click **Browse** in the section.
- 5 Browse to the location where you stored the ISO image of the Web Gateway appliance software and click **Connect**.  
  
The ISO image becomes available for installation.
- 6 Follow the instructions for installing Web Gateway that appear on the monitor you connected to the enclosure.

When the installation is completed, you can log on to the user interface of Web Gateway.

For information about the logon and how to continue, see the *Setting up Web Gateway* chapter in this guide.

---

## Network setup for Web Gateway on a blade server

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

You can configure one of the following setups:

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

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

### Proxy HA on a blade server

You can configure the proxy HA (High Availability) mode for Web Gateway on a blade server. This mode provides the functions of a proxy that runs in explicit proxy mode combined with High Availability functions.

### Network configuration

As this is a High Availability configuration, there must be multiple instances of Web Gateway on blade servers that run as nodes in this configuration. There must be at least two director nodes, so a failover can be performed in case one of them is down. A director node directs data packets to the nodes that scan the data in a suitable manner to enable load balancing.

We recommend that you configure the proxy HA mode as a *two-legged proxy solution*. This means the following is configured on a director node:

- Network interface for inbound web traffic
- Network interface for outbound web traffic

The network interface that handles inbound traffic must have a virtual IP address of its own. The network interface for outbound web traffic should also be used to do the load balancing. This is achieved by specifying its IP address as the physical component that is configured together with the management IP address.

We also recommend that you configure the following on each director node:

- Network interface for out-of-band management

Configuring this network interface allows you to perform management communication separately.

- Network interface for internal communication within the blade system enclosure

This network interface has its IP address configured under VRRP (Virtual Router Redundancy Protocol).

### Link resilience

If switches are installed as interconnect modules on an enclosure, link resilience can be achieved in the following way:

- Two of the ports used as *uplink ports* on a switch are bundled in a trunk group.
- Each of these ports is connected by a network cable to a physical link.

This means that if one the two links fails, the trunk group remains still active.

The interconnect modules and the trunk groups are mapped to the ports on the network interfaces, for example, as shown in the following table. For the network interface that handles internal communication, no port mapping to a trunk group is required.

**Table 5-1 Mapping of network components in a proxy HA configuration**

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

For more information on how to configure the interconnect modules, refer to the *GbE2c Ethernet Blade Switch for c-Class BladeSystem Application Guide* that is available on the website of the McAfee partner.

### Proxy with external load balancing on a blade server

You can configure the explicit mode for Web Gateway on a blade server with load balancing performed by an external device.

#### Network configuration

We recommend that you configure a *two-legged proxy solution* for this mode, with two separate network interfaces on each blade server for inbound and outbound web traffic. Each of these interfaces is configured with an IP address of its own.

Additionally, a network interface for out-of-band management should be configured, which allows you to perform also management communication separately.

#### Load balancing

Load balancing is performed in this configuration not by one of the blade servers, but by an external load balancer, which directs load to the blade servers. For this purpose, the blade servers are included in a load balancing pool.

When configuring the load balancer, an algorithm can be configured that supports IP client stickiness. This ensures that functions requiring IP client stickiness are available, for example, a progress page.

### Link resilience

If switches are installed as interconnect modules on an enclosure, link resilience can be achieved in the following way:

- Two of the ports used as *uplink ports* on a switch are bundled in a trunk group.
- Each of these ports is connected by a network cable to a physical link.

This means that if one the two links fails, the trunk group remains still active.

The interconnect modules and the trunk groups are mapped to the ports on the network interfaces, for example, as shown in the following table.

**Table 5-2 Mapping of network components in an explicit proxy configuration with external load balancing**

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

For more information on how to configure the interconnect modules, refer to the *GbE2c Ethernet Blade Switch for c-Class BladeSystem Application Guide* that is available on the website of the McAfee partner.

## Transparent modes on a blade server

You can configure transparent modes for Web Gateway on a blade server.

In these modes, Web Gateway runs as a transparent router that directs data packets between segments of your network or serves as a transparent bridge that allows the transferring of data packets between these segments.

### Transparent router

We recommend that you configure the transparent router mode as a *two-legged proxy solution*, with two separate network interfaces for inbound and outbound web traffic.

Each of the network interfaces is configured with its own IP address under VRRP (Virtual Router Redundancy Protocol).

The outbound network interface should be used for load-balancing the traffic. This is achieved by specifying its IP address as the physical component that is configured together with the management IP address.

If IP spoofing is configured, the blade servers on which Web Gateway only scans web traffic, without also directing it, do not need a connection for inbound web traffic. Inbound and outbound traffic is handled by an instance of Web Gateway that runs as a director node on a blade server.

### Transparent bridge

We recommend that you configure also the transparent bridge mode as a *two-legged proxy solution*, with two separate network interfaces for inbound and outbound web traffic.

For this network mode, the two-legged solution does not require virtual IP addresses and no communication under VRRP is performed accordingly.

When configuring the management IP address, you need to specify the IP address of the network interface that has been configured as the *ibr0* bridge interface.

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

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



When the load balancing role on a director node is assigned under STP, this protocol must be disabled on the switches not only if Web Gateway runs on a blade server, but also if it runs on an appliance box or on a virtual machine.

---

## Port assignments on a blade server

When running on a blade server, Web Gateway uses the network interfaces of this blade server. The ports that are assigned to these network interfaces are physically provided by the interconnect modules in an enclosure.

The network interfaces of a blade server are located on its system board and on additional network interface cards (Mezzanine cards). The interconnect modules that provide the ports for the network interfaces are in the interconnect bays of an enclosure.

Ports can be assigned to network interfaces, but also the relations between all the components involved in the communication on a blade server system can be mapped.



The mapping of the components in a blade server system can be viewed on the Onboard Administrator of an enclosure.

### Interconnect modules and bays

Interconnect modules in a blade server system that Web Gateway can run on can be:

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

The number of ports that can be physically provided by an interconnect module is 16 for a pass-through module and 5 for a switch. An M3 enclosure model has 4 interconnect bays, an M7 model has 8. This means the number of ports in a blade server system can vary between 20 and 128.

### Network interface and cards

There can be up to 8 network interfaces embedded on the system board and two additional (Mezzanine) cards:

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

An enclosure can hold up to 16 blade servers. This means the number of network interfaces in a blade server system can vary between 2 (only one blade server with only the system board card in an enclosure) and 128.

So all kinds of matches and mismatches between the number of ports and the number of network interfaces can occur. There can be a port for every network interface, there can be fewer ports than network interfaces, but also more.

### Mapping of network interfaces, ports, and interconnect bays

The ports for the network interfaces on a blade server are always mapped in the same way to the interconnect bays that are the locations of the interconnect modules.

For example, the port for the first network interface on the system board of a blade server is always mapped to the first interconnect bay of an enclosure.

As the M3 enclosure model only has 4 interconnect bays, 2 ports of a blade server are mapped to the same interconnect if the blade server is fully equipped with 8 network interfaces on 3 network interface cards. The mapping is not completely straightforward.

This mapping is shown in the following table:

**Table 5-3 Port mapping on M3 enclosure**

Port for network interface	Interconnect bay
System board – port 1	1
System board – port 2	1
Mezzanine card 1 – port 1	2
Mezzanine card 1 – port 2	2
Mezzanine card 2 – port 1	3
Mezzanine card 2 – port 2	4
Mezzanine card 2 – port 3	3
Mezzanine card 2 – port 4	4

On the M7 enclosure model, which has 8 interconnect bays, the mapping is as shown in the following table:

**Table 5-4 Port mapping on M7 enclosure**

Port for network interface	Interconnect bay
System board – port 1	1
System board – port 2	2
Mezzanine card 1 – port 1	3
Mezzanine card 1 – port 2	4
Mezzanine card 2 – port 1	5
Mezzanine card 2 – port 2	6
Mezzanine card 2 – port 3	7
Mezzanine card 2 – port 4	8

## Port assignments

The following table shows the ports that are assigned to the network interfaces on a G6 blade server model and the names of the network interfaces that are used by the operating system.

The network interface card models are also shown.

**Table 5-5 Port assignments on G6 blade server**

Card model	Port for network interface	Interface name of the operating system
HP NC 352i	System board – port 1	eth6
	System board – port 2	eth7
HP NC 360m	Mezzanine card 1 – port 1	eth0
	Mezzanine card 1 – port 2	eth1
HP NC 364m	Mezzanine card 2 – port 1	eth2

**Table 5-5 Port assignments on G6 blade server** *(continued)*

Card model	Port for network interface	Interface name of the operating system
	Mezzanine card 2 – port 2	eth3
	Mezzanine card 2 – port 3	eth4
	Mezzanine card 2 – port 4	eth5

The next table shows the port assignments on the G6.5 blade server model.

**Table 5-6 Port assignments on G6.5 blade server**

Card model	Port for network interface	Interface name of the operating system
HP NC 352i	System board – port 1	eth6
	System board – port 2	eth7
HP NC 382m	Mezzanine card 1 – port 1	eth4
	Mezzanine card 1 – port 2	eth5
HP NC 364m	Mezzanine card 2 – port 1	eth0
	Mezzanine card 2 – port 2	eth1
	Mezzanine card 2 – port 3	eth2
	Mezzanine card 2 – port 4	eth3

The last table shows the port assignments on the G8 blade server model.

**Table 5-7 Port assignments on G8 blade server**

Card model	Port for network interface	Interface name of the operating system
HP NC 352i	System board – port 1	eth0
	System board – port 2	eth1
HP NC 360m	Mezzanine card 1 – port 1	eth2
	Mezzanine card 1 – port 2	eth3
HP NC 364m	Mezzanine card 2 – port 1	eth4
	Mezzanine card 2 – port 2	eth5



# Index

## A

- about this guide [5](#)
- activate product [19](#)
- Active System Console (ASC)
  - general [39](#)
  - install [42](#)
- appliance
  - activate product [19](#)
  - default initial configuration settings [12](#)
  - hardware administration tools [39](#)
  - log on to user interface [18](#)
  - physical [10](#)
  - pre-installed software [12](#)
  - re-image [22](#)
  - serial system console settings [23](#)
  - upgrades [9](#)
  - virtual [10](#)
- appliance volume wizard [17](#)

## B

- Baseboard Management Controller (BMC)
  - configure [41](#)
  - general [39](#)
- blade server
  - enclosure [45](#)
  - explicit proxy mode with external load balancing [52](#)
  - install blade server system [46](#)
  - install enclosure [47](#)
  - install interconnect modules [47](#)
  - install Web Gateway using external CD/DVD drive [49](#)
  - install Web Gateway using internal CD/DVD drive [49](#)
  - install Web Gateway using USB drive [50](#)
  - install Web Gateway with virtual media [50](#)
  - interconnect modules [47](#)
  - McAfee Blade [45](#)
  - port assignments [54](#)
  - prepare installation of blade server system [46](#)
  - proxy HA mode [51](#)
  - STP (Spanning Tree Protocol) [53](#)
  - supported enclosure models [45](#)
  - supported model [45](#)
  - transparent modes [53](#)
  - turn on enclosure [48](#)

## C

- cache volume resizing [17](#)
- configuration wizard
  - implement default initial configuration settings [17](#)
  - implement own initial configuration settings [17](#)
- conventions and icons used in this guide [5](#)
- copper NIC
  - 1GbE card [35](#)
  - appliance models [35](#)
  - supported types [35](#)

## D

- data collection
  - configure [19](#)
  - review Data Usage Statement [19](#)
- Data Usage Statement [19](#)
- documentation
  - audience for this guide [5](#)
  - product-specific, finding [6](#)
  - typographical conventions and icons [5](#)

## E

- End User License Agreement [19](#)

## F

- fiber NIC
  - 10GbE card [33](#)
  - 1GbE card [32](#)
  - appliance models [31](#)
  - supported types [31](#)

## H

- hardware administration tools
  - Active System Console (ASC) [39](#)
  - Baseboard Management Controller (BMC) [39](#)
  - Platform Confidence Test (PCT) [39](#)
  - Remote Management Module (RMM) [39](#)
  - SNMP Subagent (SNMP SA) [39](#)
- Hardware Security Module, *See* HSM card
- HSM card [36](#)

**L**

- licensing
  - import license [19](#)
  - review End User License Agreement [19](#)
  - temporary license key [21](#)
- logon to user interface [18](#)

**M**

- McAfee ServicePortal, accessing [6](#)
- memory upgrade [27](#)

**N**

- network interface card, See NIC
- NIC
  - copper NIC [35](#)
  - fiber NIC [31](#)

**P**

- PCI card
  - copper NIC [35](#)
  - fiber NIC [31](#)
  - HSM card [36](#)
  - install [37](#)
- Platform Confidence Test (PCT) tool
  - general [39](#)
  - install [40](#)
  - run hardware test [40](#)
- port assignments
  - blade server [54](#)
  - physical appliance [23](#)

**R**

- re-image appliance [22](#)
- release notes [9](#)
- Remote Management Module (RMM)
  - configure [41](#)
  - general [39](#)
- requirements
  - physical appliance [10](#)
  - virtual appliance [10](#)

**S**

- serial system console settings [23](#)
- ServicePortal, finding product documentation [6](#)
- setting up Web Gateway
  - activate product [19](#)
  - appliance volume wizard [17](#)
  - cache volume resizing [17](#)
  - complete procedure [18](#)
  - configure data collection [19](#)
  - configure more initial settings [20](#)
  - Data Usage Statement [19](#)
  - default initial configuration settings [12](#)

- setting up Web Gateway (*continued*)
  - download software for physical appliance [13](#)
  - download software for virtual appliance [14](#)
  - download update files [19](#)
  - high-level steps [9](#)
  - implement default initial configuration settings [17](#)
  - implement own initial configuration settings [17](#)
  - initial configuration settings [17](#)
  - install on physical appliance [13](#)
  - install on virtual appliance [15](#)
  - licensing [19](#)
  - log on to user interface [18](#)
  - memory upgrade [27](#)
  - physical appliance with downloaded software [12](#)
  - physical appliance with pre-installed software [12](#)
  - port assignments [23](#)
  - pre-installed software [12](#)
  - re-image appliance [22](#)
  - requirements [10](#)
  - serial system console settings [23](#)
  - setup wizard [18](#)
  - solve connection problems [21](#)
  - temporary license key [21](#)
  - virtual appliance [14](#)
  - virtual machine settings [15](#)
- settings
  - additional configuration [20](#)
  - default initial configuration [12](#)
  - own initial configuration [17](#)
  - serial system console [23](#)
  - virtual machine [15](#)
- setup wizard
  - activate product [19](#)
  - appearing [18](#)
  - complete setup procedure [19](#)
  - configure more initial settings [20](#)
  - Data Usage Statement [19](#)
  - End User License Agreement [19](#)
  - review online documents [19](#)
  - solve connection problems [21](#)
  - work with [18](#)
- SNMP Subagent (SNMPSA)
  - enable [42](#)
  - general [39](#)
- STP (Spanning Tree Protocol)
  - assign load-balancing role [53](#)
  - disable use on switches [53](#)

**T**

- technical support, finding product information [6](#)

**U**

- upgrading Web Gateway [9](#)

user interface  
  log on [18](#)  
  setup wizard [18](#)

## W

wizards  
  appliance volume wizard [17](#)

wizards (*continued*)  
  configuration wizard [17](#)  
  setup wizard [18](#)

