# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Welcome</td>
<td>5</td>
</tr>
<tr>
<td>New hardware platforms</td>
<td>5</td>
</tr>
<tr>
<td>2. Platforms</td>
<td>7</td>
</tr>
<tr>
<td>Appliance models</td>
<td>7</td>
</tr>
<tr>
<td>McAfee Web Gateway 4000</td>
<td>7</td>
</tr>
<tr>
<td>McAfee Web Gateway 4500</td>
<td>7</td>
</tr>
<tr>
<td>McAfee Web Gateway 5000</td>
<td>8</td>
</tr>
<tr>
<td>McAfee Web Gateway 5500</td>
<td>8</td>
</tr>
<tr>
<td>Blade server platform</td>
<td>9</td>
</tr>
<tr>
<td>3. Installation and Configuration</td>
<td>11</td>
</tr>
<tr>
<td>Installation and initial configuration</td>
<td>11</td>
</tr>
<tr>
<td>Create a configuration file</td>
<td>11</td>
</tr>
<tr>
<td>Setup utility window</td>
<td>12</td>
</tr>
<tr>
<td>Install the appliance box</td>
<td>13</td>
</tr>
<tr>
<td>Default settings</td>
<td>14</td>
</tr>
<tr>
<td>Access the user interface</td>
<td>15</td>
</tr>
<tr>
<td>Using the system CD ROM</td>
<td>15</td>
</tr>
<tr>
<td>Setup procedure</td>
<td>15</td>
</tr>
<tr>
<td>Using the USB drive</td>
<td>17</td>
</tr>
<tr>
<td>Provide initial configuration settings</td>
<td>17</td>
</tr>
<tr>
<td>Re-imaging the appliance</td>
<td>17</td>
</tr>
<tr>
<td>Port assignments</td>
<td>19</td>
</tr>
<tr>
<td>McAfee Web Gateway 4000</td>
<td>19</td>
</tr>
<tr>
<td>McAfee Web Gateway 4500</td>
<td>19</td>
</tr>
<tr>
<td>McAfee Web Gateway 5000</td>
<td>20</td>
</tr>
<tr>
<td>McAfee Web Gateway 5500</td>
<td>20</td>
</tr>
<tr>
<td>4. Diagnostic tools</td>
<td>21</td>
</tr>
<tr>
<td>Platform Confidence Tool</td>
<td>21</td>
</tr>
<tr>
<td>Active System Console</td>
<td>22</td>
</tr>
<tr>
<td>Remote Management Module and Baseboard Management Controller</td>
<td>22</td>
</tr>
<tr>
<td>SNMP Subagent</td>
<td>23</td>
</tr>
<tr>
<td>5. Providing a Microsoft certificate</td>
<td>25</td>
</tr>
<tr>
<td>Creating a Microsoft certificate</td>
<td>25</td>
</tr>
<tr>
<td>Implementing a Microsoft certificate</td>
<td>29</td>
</tr>
</tbody>
</table>
1 Introduction

Welcome

Welcome to the McAfee® Web Gateway Installation and Configuration Guide. It provides you with the information on the McAfee Web Gateway appliance models.

Each model uses a different server system as the hardware platform for the McAfee Web Gateway appliance software. There is also the option of using the McAfee Content Security Blade Server as a platform.

New hardware platforms

New server systems have been introduced as hardware platforms for use with subversion 6.8.7 C and higher versions of McAfee Web Gateway. The appliance software for McAfee Web Gateway can be installed to run on any of these systems.
Introduction
New hardware platforms
2 Platforms

Contents
Appliance models
Blade server platform

Appliance models

The various models of the McAfee Web Gateway appliance are listed below with the main features that are provided by the new hardware platforms.

McAfee Web Gateway 4000

The main features of this appliance model are as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form factor</td>
<td>1U</td>
</tr>
<tr>
<td>Rack mount</td>
<td>yes</td>
</tr>
<tr>
<td>Processor</td>
<td>Dual Core Celeron E3400</td>
</tr>
<tr>
<td>Memory</td>
<td>2 x 2 GB DDR2 ECC</td>
</tr>
<tr>
<td>Hard disk</td>
<td>500 GB SATA</td>
</tr>
<tr>
<td>Network interfaces</td>
<td>3 RJ-45 Gigabit Ethernet</td>
</tr>
<tr>
<td>USB interfaces</td>
<td>5 USB 2.0</td>
</tr>
<tr>
<td>Serial interface</td>
<td>DB-9 Port A</td>
</tr>
<tr>
<td>Power supply</td>
<td>single 350 W</td>
</tr>
</tbody>
</table>

For more information, refer to the Intel Server System SR 1530 SH Technical Product Specification.

Note: For this appliance model, the hardware platform provides a Celeron processor (as stated in the above table and differing from the Intel Server System SR 1530 SH Technical Product Specification).

McAfee Web Gateway 4500

The main features of this model are as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form factor</td>
<td>1U</td>
</tr>
<tr>
<td>Rack mount</td>
<td>yes</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel Core i3 540 3.07 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>2 x 2 GB DDR3 ECC</td>
</tr>
<tr>
<td>Hard disks</td>
<td>2 x 300 GB SAS 3.5 inch RAID 1 without buffer backup</td>
</tr>
<tr>
<td>Network interfaces</td>
<td>5 RJ-45 Gigabit Ethernet</td>
</tr>
<tr>
<td>USB interfaces</td>
<td>5 USB 2.0</td>
</tr>
<tr>
<td>Serial interface</td>
<td>RJ-45</td>
</tr>
<tr>
<td>Power supply</td>
<td>single 350 W</td>
</tr>
</tbody>
</table>

For more information, refer to the Intel Server System SR 1630 HGPRX Technical Product Specification.
McAfee Web Gateway 5000

The main features of this model are as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form factor</td>
<td>1U</td>
</tr>
<tr>
<td>Rack mount</td>
<td>yes</td>
</tr>
<tr>
<td>Processor</td>
<td>Xeon E5640</td>
</tr>
<tr>
<td>Memory</td>
<td>3 x 2 GB DDR3 ECC</td>
</tr>
<tr>
<td>Hard disks</td>
<td>2 x 300 GB SAS 2.5 inch RAID 1 with battery backup</td>
</tr>
<tr>
<td>Network interfaces</td>
<td>4 RJ-45 Gigabit Ethernet</td>
</tr>
<tr>
<td>USB interfaces</td>
<td>5 USB 2.0</td>
</tr>
<tr>
<td>Serial interface</td>
<td>RJ-45 Port A</td>
</tr>
<tr>
<td>Power supply</td>
<td>2 x 650 W hot-swap</td>
</tr>
</tbody>
</table>

For more information, refer to the *Intel Server System SR 1625 URSASRNA Technical Product Specification*.

McAfee Web Gateway 5500

The main features of this model are as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form factor</td>
<td>2U</td>
</tr>
<tr>
<td>Rack mount</td>
<td>yes</td>
</tr>
<tr>
<td>Processor</td>
<td>2 Xeon X5660</td>
</tr>
<tr>
<td>Memory</td>
<td>6 x 2 GB DDR3 ECC</td>
</tr>
<tr>
<td>Hard disks</td>
<td>6 x 300 GB SAS RAID 10 with battery backup</td>
</tr>
<tr>
<td>Network interfaces</td>
<td>4 RJ-45 Gigabit Ethernet</td>
</tr>
<tr>
<td>USB interfaces</td>
<td>5 USB 2.0</td>
</tr>
<tr>
<td>Serial interface</td>
<td>RJ-45 Port A</td>
</tr>
<tr>
<td>Power supply</td>
<td>2 x 780 W hot-swap</td>
</tr>
</tbody>
</table>

For more information refer to the *Intel Server System SR 2625 URLXRNA Technical Product Specification*. 
Blade server platform

Instead of running McAfee Web Gateway on the hardware platforms described in the preceding sections, you can also use version 5.3 of the McAfee Content Security Blade Server as a platform.

When using this option, make sure the McAfee Web Gateway version you install is subversion 6.8.5 D or a higher version.

The McAfee Content Security Blade Server is the highest capacity model within the McAfee Messaging and Web Security product range, designed to scan Web and email traffic for viruses, spam, and many other threats to your network.

This blade server product:

- Scans and processes HTTP, ICAP, and FTP traffic (Web security software).
- Scans and processes SMTP and POP3 messaging traffic (email security software).
- Reduces the cost of storing and running standalone appliances in your datacenter.
- Is scalable. You can add more blades to increase the scanning throughput without compromising performance.
- Is easy to manage and administer. It balances the scanning workload and updates the detection definition (DAT) files across the blades.
- Has built-in workload management. If you already use a load balancer in your network, you can leave it there when you install the blade server, even though it is no longer required to balance the scanning workload.

The blade server includes different types of blade components:

- A management blade for managing network traffic and passing it on to the content scanning blades, using its internal workload management. It is not used itself as a content scanning blade.
- A failover management blade, which is identical to the management blade. It takes over the management functions should the primary management blade fail.
- Content scanning blades used to scan traffic for dangerous or inappropriate content. The blade server can be run with one content scanning blade as a minimum.

For more information, refer to the McAfee Content Security Blade Server 5.3 Installation Guide.
Platforms
Blade server platform
Installation and initial configuration

This section tells you how to install your McAfee Web Gateway appliance on a hardware platform and perform the initial configuration.

Note: For information on how to install McAfee Web Gateway on a blade server, refer to the McAfee Content Security Blade Server 5.3 Installation Guide.

During the installation procedure, you can provide the appliance with your own initial configuration settings. It is highly recommended that you do this because if you do not provide your own settings, the appliance will be configured with the default settings, which are usually impracticable in any particular environment.

Using the system CD ROM that is shipped with the appliance, you can also repeat parts of the installation procedure. This enables you to modify the initial settings, see Using the system CD ROM.

To provide your own initial configuration settings, which include host and server names, IP addresses, and other information, you need to create a configuration file. A setup utility is provided for this purpose.

You can store this file on a floppy disk and insert it in the floppy disk drive of the appliance box if it is equipped with one. Alternatively, you can use a USB drive to transfer the settings on to the appliance.

When the appliance is turned on, it will be initially configured with these settings.

Create a configuration file

A setup utility is included on the system CD ROM to assist you in providing initial configuration settings for your appliance. Proceed as follows:

1. Insert the system CD ROM in a suitable drive of a Microsoft Windows PC.
2. Start the utility. Its name is WWAppSetup.exe.
   Starting the utility opens a window that provides a number of input fields.
3. After entering the appropriate data, click the Write button in the window.
   The utility then generates the config.xml configuration file.
4. You can store this file in the root directory of a floppy disk that has been formatted to provide a Microsoft-style file system and insert it in the floppy disk drive of your appliance box if it is equipped with one. Alternatively, you can store the file on a USB drive and connect it to the appliance before turning it on.
Setup utility window

When the setup utility is started, it displays the following window:

![Setup utility window screenshot](image)

The meaning of the items in this window is as follows:

- **Host Name** — Input field for entering the name of the system that the appliance is running on
  
  *Default*: `wwapp`

- **First LAN Interface (eth0)** — Area for entering data to specify the first of two LAN interfaces

  - **Activate on Boot** — Select this checkbox to activate this interface after booting the appliance.
    
    *Default*: The checkbox is selected.

  - **IP Address** — IP address for this interface
    
    *Default*: 192.168.0.222

  - **Network Mask** — Network mask for this interface.
    
    *Default*: 255.255.255.0
Installation and initial configuration

- **Second LAN Interface (eth1)** — Area for entering data to specify the second of two LAN interfaces
  - **Activate on Boot** — Select this checkbox to activate this interface after booting the appliance.
    
    *Default:* The checkbox is selected.
  - **IP Address** — IP address for this interface
    
    *Default:* 192.168.0.223
  - **Network Mask** — Network mask for this interface.
    
    *Default:* 255.255.255.0
  - **Gateway IP Address** — IP address of the gateway where the appliance is running.
  - **First Name Server** — IP address of the first of two domain name servers called on by the appliance
  - **Second Name Server** — IP address of the second of two domain name servers called on by the appliance
  - **Permit SSH Login as root** — Select this checkbox to allow the use of `ssh` for logging in as root user.
    
    *Default:* The checkbox is deselected.
  - **Write** — After entering the configuration settings in the input fields, click this button.
    
    The setup utility will then create a `config.xml` configuration file.
  - **Cancel** — Click this button to leave the setup utility without creating a configuration file.

**Install the appliance box**

To install the appliance box, proceed as follows:

1. Connect the power supply cable to the power supply connector on the rear side of the appliance box.

2. If you want to have messages concerning the appliance status displayed:
   
   Connect the appliance box to a standard VGA monitor or a serial console. On the appliance box, connect the monitor cable to one of the video connectors on its front or rear side.
   
   *Note:* You need to connect the appliance box to this monitor in order to receive messages when you are performing parts of the installation procedure again, using the system CD ROM, see *Using the system CD ROM*.

3. Implement your initial configuration settings.
   
   To do this, insert a floppy disk containing these settings in the floppy disk drive on the front side of the appliance box if it is equipped with one. Alternatively, you can use a USB drive to transfer the settings on to the appliance.
   
   The configuration settings are then read and implemented. A lock file is created for this purpose. It is stored under `/var/lock/cgconfig`.
   
   Reading and implementing the settings of the `config.xml` configuration file is then omitted at every subsequent boot. Unless a `config.xml` configuration file has been read successfully, an attempt is made to do so at every boot.
   
   If you want to enforce reading of the `config.xml`, delete the lock file. No new installation procedure is required for this.

4. Turn the appliance box on, using the power switch on its front side.
   
   The initial configuration settings that provided are now implemented on the appliance.

After completing these steps, you can go on to access the user interface. If you wish to repeat parts of the installation procedure, you can do this using the system CD ROM, see *Using the system CD ROM*. 
Default settings

The appliance is shipped with the default settings that are described in the following.

General settings

A McAfee Web Gateway appliance is by default set to these values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of NIC 1</td>
<td>192.168.0.222</td>
</tr>
<tr>
<td>Admin account (for login to the user interface)</td>
<td>admin</td>
</tr>
<tr>
<td>Admin password (for login to the user interface)</td>
<td>webwasher</td>
</tr>
<tr>
<td>Administration port (for login to the user interface)</td>
<td>10000 (https)</td>
</tr>
<tr>
<td>System administration account</td>
<td>root</td>
</tr>
<tr>
<td>System administration password</td>
<td>not enabled</td>
</tr>
</tbody>
</table>

Serial interface settings

You can use the serial interface at the rear side of an appliance box to connect it to a console. This interface is by default set to these values:

192008N1

The meaning of these settings is as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit rate</td>
<td>19200</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>none</td>
</tr>
<tr>
<td>Stop bit</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>not enabled</td>
</tr>
</tbody>
</table>

After completing the installation procedure, you can login to the appliance via this console as root user. The initial password consists of the last 8 digits of the MAC address for the first onboard NIC, see label affixed to the box. All letters in this address are written in capitals. It is recommended to change the initial password after using it for the first login.

You can also use one of the video connectors at the front or rear side of an appliance box to connect it to a serial or a VGA terminal. You can then login to the appliance with the same user name and password as from a console connected to the serial interface.

The terminal used for this connection should be a standard VGA or VT100 compatible device.

A remote login with ssh, which runs on an appliance by default, can also be performed if you have configured the corresponding option in the config.xml configuration file.
Access the user interface

After completing the installation and initial configuration, you should be able to connect to the user interface of the McAfee Web Gateway appliance from any browser that has access to the network segment of the appliance.

Proceed as follows:

1. Point your browser to:
   
   https://<ip address>:10000

   where <ip address> is the address you selected when using the setup utility to provide your initial configuration settings, or 192.168.0.222 if you started the appliance using the default settings.

2. Login as admin — the default password is webwasher.

3. This will open the Home page of the user interface. On this page, first upload the license key file, which you should have received by e-mail. Please contact the McAfee customer service if you did not receive this license key file.

Some expert settings, such as customization of the user error templates, require access to the file system of the appliance. You can connect to this system by using an ssh client to connect to the IP address of the appliance.

To login as root, use the password that is built from the last eight digits of the MAC address for the first onboard network interface, see the label affixed to the appliance box. The letters in this password must all be capitals.

The user interface provides various tabs for completing further configuration tasks, which can be accessed under Configuration > Appliance.

For a description of these tasks, see the McAfee Web Gateway System Configuration Administration Guide.

Using the system CD ROM

The operating system and the McAfee Web Gateway (formerly Webwasher®) software are provided on a bootable system CD ROM, which is delivered with the appliance box.

You can use this medium to repeat parts of the installation procedure.

When booting from the system CD ROM, the hard disk is partitioned, the operating system together with the application software is installed, and the system configuration is started.

This process runs automatically, and there is no need for you to intervene. At a later stage of the process, you will be prompted by messages on the monitor that has been connected to the appliance box.

Note that the configuration settings are implemented at the first boot.

Setup procedure

To install the operating system and the McAfee Web Gateway software using the system CD ROM, complete the following steps:

1. Insert the system CD ROM in the CD ROM drive on the front side of the appliance box.

   The system CD ROM begins with the boot process. Messages concerning its progress are displayed on the monitor that is connected to the appliance box.

2. At one time, you will see a message like the following, asking you to select the serial or the video console, to continue the boot process:

   Webwasher Appliance %s Installer. Press RETURN to start.

   1 serial console preferred
2 video console preferred (default)

boot:

where $v$ is the version of your appliance.

Enter 1 or 2 for your preferred option after boot: and press Return on your keyboard.

If you do no enter a value, the default will be taken after a timeout interval has elapsed, which is that the serial console is preferred.

When the boot process is continued, a warning is displayed that the installation process will perform a partitioning of the hard disk for the system that it is running on.

You are informed that you have 25 seconds time to remove the system CD ROM, in case you do not want this to happen.

A situation where you may want to remove the system CD ROM may arise when you have unintentionally inserted it in the wrong system, or inserted it only for reading document files, but not for performing an installation.

Then the hard disk is partitioned, the operating system and the application software are installed, and the system configuration is started. There is no need for you to intervene at this stage of the process.

When this process has finished successfully, you are informed about it by a corresponding message.

3 The system CD ROM ejects automatically, and you are asked to remove it. This is followed by a message asking you to reset the appliance.

Remove the system CD ROM.

4 If you want to have your own initial configuration settings implemented rather than the default settings:

Insert a floppy disk with these settings in the floppy disk drive on the front side of the appliance box if it is equipped with one.

Alternatively, you can use a USB drive to transfer the settings on to the appliance.

5 Reset the appliance by pressing the Reset button on the front side of the appliance box. If there is no reset button on your appliance box model, use the Power on/off button to reset the appliance.

6 When performing the reset, the system continues with the configuration process, making use of the config.xml configuration file if there is one available.

After the reset, a number of lines providing system information are displayed. This completes the installation and configuration process.

7 If you have inserted a disk or USB drive, remove it.

After you have completed these steps, you can go on to access the user interface. It enables you to complete further configuration tasks.
Using the USB drive

The USB drive that is shipped with your McAfee Web Gateway appliance can be used for performing various tasks.

You can use this flash drive device, which is also known as USB stick, to provide your own settings for the initial configuration of the appliance instead of the default settings.

You can also use it to re-image the appliance. Be aware, however, that this will overwrite all data stored there.

When re-imaging the appliance you can either use the image that is pre-installed on the drive, or download a new image from the Extranet for McAfee Web Gateway, copy it to the drive, and use it for re-imaging.

The latter procedure may also help you in case you have lost the shipped drive. You can follow it to download a new image and copy it to a new drive.

**Note:** Not every type of USB drive is suitable for booting a McAfee Web Gateway appliance. It is therefore generally recommended to use only drives provided by McAfee for this purpose.

Provide initial configuration settings

The appliance is shipped with the McAfee Web Gateway software pre-installed. You can use the USB drive, however, to configure your own initial settings for host name, interfaces, and other parameters, instead of the default settings.

Complete the following steps to do this:

1. Insert the USB drive in a Windows-based appliance or workstation. The file manager then assigns the drive a unique drive letter.

2. Browse this drive and start the WWAppSetup.exe configuration tool.

3. Use the tool to specify your initial configuration settings.

4. Click the **Write** button provided by the tool to write these settings into the config.xml configuration file.

5. Store the file on the USB drive directly under root (not in a subordinate folder).

6. Insert the drive into one of the appliance’s USB ports.

7. Turn on the appliance.

   The appliance boots and uses the settings in the config.xml file. Note that you can add a config.xml only once this way since it is stored and read at every reboot.

Re-imaging the appliance

You can also use the USB drive to re-image your appliance. Note, however, that this will overwrite all data stored there.

You may either use the image that is already on the drive, or download another image from the Extranet for McAfee Web Gateway and install it on your appliance.

Use the pre-installed image

If you want to use the image that is pre-installed on the USB drive for re-imaging your appliance, proceed as follows:

1. Connect a monitor and keyboard to your appliance.

2. Insert the USB drive into one of the appliance’s USB ports.

3. Turn on the appliance.

4. When prompted, press **F2** to enter the setup menu.
5 Navigate to the **Boot Manager** submenu, select the USB drive option, and press **Enter** on your keyboard.

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

The installation program continues with a menu for configuring the video output device. After completing all steps, the appliance boots and the McAfee Web Gateway software is installed from the USB drive.

You can implement a **config.xml** when re-imaging the appliance by storing the file on the drive before inserting it.

**Use another image**

If you want to use another image for re-imaging your appliance than the one that is pre-installed on the USB drive, you need to go to the Extranet for McAfee Web Gateway and download the image you want to use.

Then this image must be copied to the drive. Tools are provided for this purpose under Windows and Linux. You can also use this procedure to copy an image to a new drive in case you have lost the one that was shipped to you.

Note, however, that not every type of USB drive is suitable for booting a McAfee Web Gateway appliance, and that it is generally recommended to use only drives provided by McAfee for this purpose.

Complete the following steps to re-image your appliance with another image than the one that is pre-installed:

1 Login to the Extranet for McAfee Web Gateway and download a USB image to your system.

   Note that you need to download one of the images that are provided especially for installation with the USB drive, not an ordinary ISO image.

   The file name extension for this USB image should be **.usb**.

2 Copy the downloaded image to the USB drive.

   You may, for example, use the **dd** tool to do this, which is provided with your Linux distribution. For Windows, it may be obtained from the Chrysocome Web site under the terms of a GPL license, see [http://www.chrysocome.net/dd](http://www.chrysocome.net/dd).

   The command syntax that is required for copying the image with this tool is given below. Note that you need to be logged in as root administrator in order to be able to use the command.

   Note, furthermore, that the copy operation will completely overwrite everything that was stored on the drive.

   If you want to preserve your old **config.xml** configuration file, you need to save it before you do the re-imaging and copy it back to the drive afterwards, in order to be able to use the drive for rebooting your appliance with your individual configuration settings.

   The general syntax of the **dd** command is:

   ```
   dd if=<USB image> of=<USB device> bs=16k
   ```

3 Connect a monitor and keyboard to your appliance.

4 Insert the USB drive with the new image into one of the appliance’s USB ports.

5 Turn on the appliance.

6 When prompted, press **F2** to enter the setup menu.

7 Navigate to the **Boot Manager** submenu, select the USB drive option, and press **Enter** on your keyboard.

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

The installation program continues with a menu for configuring the video output device. After completing all steps, the appliance boots and the new image is installed from the USB drive.
Port assignments

Ports are assigned to the network interfaces on each appliance model as shown in the following.

**McAfee Web Gateway 4000**

This model has three network interfaces.

<table>
<thead>
<tr>
<th>Position</th>
<th>Network Interface</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>e1000e eth1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>e1000 eth0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>e1000e eth2</td>
<td></td>
</tr>
</tbody>
</table>

**McAfee Web Gateway 4500**

This model has five network interfaces.

<table>
<thead>
<tr>
<th>Position</th>
<th>Network Interface</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>igb eth1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>igb eth2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>igb eth3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>igb eth4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>e1000e eth0</td>
<td></td>
</tr>
</tbody>
</table>
McAfee Web Gateway 5000

This model has four network interfaces.

Ports are assigned to these interfaces as follows:

<table>
<thead>
<tr>
<th>Position</th>
<th>Network Interface</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>igb</td>
<td>eth2</td>
</tr>
<tr>
<td>2</td>
<td>igb</td>
<td>eth3</td>
</tr>
<tr>
<td>3</td>
<td>e1000e</td>
<td>eth1</td>
</tr>
<tr>
<td>4</td>
<td>e1000e</td>
<td>eth0</td>
</tr>
</tbody>
</table>

McAfee Web Gateway 5500

This model has four network interfaces.

Ports are assigned to these interfaces as follows:

<table>
<thead>
<tr>
<th>Position</th>
<th>Network Interface</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>igb</td>
<td>eth2</td>
</tr>
<tr>
<td>2</td>
<td>igb</td>
<td>eth3</td>
</tr>
<tr>
<td>3</td>
<td>e1000e</td>
<td>eth1</td>
</tr>
<tr>
<td>4</td>
<td>e1000e</td>
<td>eth0</td>
</tr>
</tbody>
</table>
Platform Confidence Tool

The Platform Confidence Test tool (PCT) assists you in detecting hardware errors. For each appliance model, there is a particular version of the tool.

You can download the appropriate version from the McAfee Extranet for Web Gateway. You can then use a USB drive to run it on your appliance in EFI (Enhanced Firmware Interface) shell mode.

Complete the following procedure to retrieve diagnostic information with the Platform Confidence Tool:

1. Download the appropriate tool version from the McAfee Extranet for Web Gateway. Tool versions are available there in zipped format.
2. Extract the content of the downloaded zip file into the root directory of a USB drive. The drive must be formatted in Microsoft DOS mode.
3. Attach the USB drive to your appliance.
4. Restart the appliance.
5. When prompted, press F2 to enter the setup menu.
6. Navigate to Server Management | Console Redirection and make sure Console Redirection is disabled.
7. Navigate to Boot Manager and select EFI Shell.

The appliance is restarted in EFI shell mode. EFI runs the startup.nsh procedure from the USB drive and displays a diagnostics menu.

Note: Pressing F10 terminates the diagnostic cycle.

8. Select a test type.

Note: The network test requires that the appliance is not plugged in to any network. To test the network interface ports, you can connect any port to another 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.

Note: It is recommended that after the comprehensive or comprehensive looping test you do a full AC power cycle (by removing power from the system) before continuing. This resets all controllers and ensures they are running in an expected mode.

9. Copy the result.log file to the USB drive:
   a. Run the map command.
   b. Identify your USB drive in the list that is displayed.
Active System Console

The Active System Console (ASC) is a web-based debugging tool. It provides information on hardware errors that are detected by the BMC through accessing the system event log and sensor data records on your appliance.

The tool also enables you to send hardware data to McAfee support. Furthermore, it allows you to configure some BMC functions, such as the IP address or trap and email communication.

Complete the following procedure to retrieve diagnostic information with the Active System Console:

1. On a system console, run the following command:
   
   ```
   asc-enable
   ```

2. When prompted, create an administrator password.
   
   **Note:** If a message on strong password setting is displayed, respond according to your requirements.

   After the password has been set, ASC is started.

3. Use a web browser to access the ASC user interface under:
   
   ```
   https://<IP address of your appliance>:9393
   ```

   When the appliance is started next time, ASC is automatically started with it. To disable ASC, use the `asc-disable` command.

   For more information, see the help information on the ASC user interface and the user documentation that is provided with the new hardware platforms.

Remote Management Module and Baseboard Management Controller

The Remote Management Module (RMM) is available on the WG5000 and WG5500 appliances. Its current version is RMM3. The tool provides functions for remote access to the appliance system and monitoring key functions.

Together with this tool, you can set up the Baseboard Management Controller (BMC), which delivers information that is used both by the Remote Management Module and the Active Console System.

The user interface of the Remote Management Module includes tabs for system overview, server health, and other monitoring functions.

On the Remote Console tab, you find a remote access console, which you can use for completing remote jobs, for example, LOM (Lights Out Management) jobs. The console also allows you to mount local drives remotely or distribute ISO images.

The console is completely Java-based. It works well on Microsoft Windows and Linux operating systems, but not on the Apple MAC OSX. The systems you want to access from the console must have Java Runtime Environment (JRE) version 1.6 installed.

Complete the following procedure to set up the Remote Management Module and Baseboard Management Controller:

1. Connect the RMM and BMC on the rear panel of your appliance box to the network.

2. Restart the appliance.

3. During the start phase, press F2. The setup menu appears.
4 Go to **Server Management** and select **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**, 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 access to the Remote Management Module.

8 Press **F10** and in the dialog window that appears, click **Yes** to save your changes.

The Remote Management Module is now available for system management activities. You can access the tool through the IP address you configured.

For information on where the RMM and BMC interfaces are located on the rear panels of the WG5000 and WG5500 appliance boxes, see the *McAfee Web Gateway Port Identification Guide*.


---

**SNMP Subagent**

When SNMP (Simple Network Management Protocol) monitoring is configured on your appliance, you can use the SNMP Subagent to retrieve additional information on hardware parameters, such as general status and sensor values.

The SNMP Subagent provides object IDs (OIDs) that belong to a MIB (Management Information Base) tree structure for hardware items. These can be queried using the SNMP functions on your appliance.

To enable the subagent, run the following command from a system console:

`snmpsa-enable`

**Note:** Running this command can cause the appliance to stop processing web traffic for a few seconds.

To disable the subsagent, use the `snmpsa-disable` command.
Providing a Microsoft certificate

Contents
Creating a Microsoft certificate
Implementing a Microsoft certificate

Creating a Microsoft certificate

You can create a Microsoft certificate for use on the McAfee Web Gateway appliance.

Complete the following procedure

1. Use your browser to go to the Microsoft Certificate Services welcome page:
2 Select Request a certificate, and from the page that is displayed select Advanced certificate request. Enter the information needed for generating the certificate as shown below (making sure Subordinate Certification Authority is selected):

![Microsoft Certificate Services screenshot](image.jpg)

3 Select Create and submit a request to this CA.

4 When you are prompted to install the certificate, follow the installation instructions that are displayed.
5 After completing the installation, go to Internet Options > Content > Certificates, where you should see the certificate installed:

6 Click Export, and in the window of the Certificate Export Wizard that opens, select Yes, export the private key. Then click Next.

7 In the next window, select Include all certificates in the certification path if possible:
8 Click **Next**.

9 When you are prompted to enter a password, enter one and click **Next**.

10 You are then prompted to save the certificate file. Click **Save**, and the certificate will be saved as .pxf file, together with a key file, which is also in .pxf format.

The wizard displays a completion window:

![Certificate Export Wizard](image)

11 Click **Finish**.

This completes the activities that are required on the Microsoft side for providing the certificate. You can now use this certificate on your McAfee Web Gateway appliance.
Implementing a Microsoft certificate

To implement a Microsoft certificate that you created for use on your McAfee Web Gateway appliance, proceed as follows:

1. Transfer the .pxf files that contain the Microsoft certificate and key to the appliance file system. You can use a utility such as WinSCP to do this.

2. Export the .pxf files to the formats that are required for importing them onto the appliance. This can be done using OpenSSL commands.

   The following command will export the certificate file to .crt format:
   
   ```bash
   ```

   This command will export the key file to .key format:
   
   ```bash
   openssl pkcs12 -in SecureWeb.pfx -cacerts -nodes -out SecureWeb.key
   ```

3. Use WinSCP to transfer the .crt and .key files generated with the OpenSSL commands in step 2 to your local system.

4. Import the certificate and key files for use on your McAfee Web Gateway appliance. To do this, browse to these files, using the buttons provided in the Import Certificate Authority section:

   a. Under Certificate, browse to the location where you stored the certificate file generated by the Microsoft Certificate Service, after exporting it to the .crt format.

   b. Under Private Key, browse to the location where you stored the key file generated by the Microsoft Certificate Service, after exporting it to the .key format. This is a password-protected file. The password is the one you entered when prompted in Step 9.

   c. Under Certificate Chain, browse to the location where you stored the certificate file of the Webwasher Root CA, after downloading it.

After browsing to the appropriate file locations, click Import.