

McAfee Firewall Enterprise, Multi-Firewall Edition

version 8.3.x

This quick start guide provides high-level instructions for setting up McAfee[®] Firewall Enterprise, Multi-Firewall Edition (hereinafter Firewall Enterprise, Multi-Firewall Edition).

- 要查看本文档的简体中文版，请访问 www.mcafee.com 然后选择语言。单击企业用户 | 支持 | 产品文档。
- Pour afficher ce document en français, rendez-vous sur le site www.mcafee.com et sélectionnez la langue de votre choix. Sélectionnez **Pour les entreprises | Support | Documentation produit**.
- Um dieses Dokument auf Deutsch anzusehen, gehen Sie zu www.mcafee.com, und wählen Sie Ihre Sprache aus. Wählen Sie **Geschäftlich | Unterstützung | Produktdokumentation**.
- このドキュメントを日本語で表示するには、www.mcafee.com で言語を選択してください。ビジネス向け | サポート | 製品マニュアルを選択します。
- Para ver este documento en español, visite www.mcafee.com y seleccione su idioma. Seleccione **Para empresas | Soporte | Documentación del producto**.

1 Check your shipment

Make sure your shipment includes these items:

- Firewall Enterprise, Multi-Firewall Edition appliance
- Rack mount kit
- Firewall software DVD
- Activation certificate
- Accessories itemized on the contents sheet

2 Download product documentation

Download the product documents.

- a Go to the McAfee Technical Support ServicePortal at mysupport.mcafee.com.
- b Under **Self Service**, click **Product Documentation**.
- c Select the appropriate product and version.

- d Download these documents.
- *McAfee Firewall Enterprise Product Guide*
 - *McAfee Firewall Enterprise, Multi-Firewall Edition Installation Guide*
 - *McAfee Firewall Enterprise Hardware Product Guide* for your model
 - *McAfee Firewall Enterprise Hardware Component Product Note*



A FIPS configuration guide is available when the product has completed the certification process.

3 Plan your configuration

Plan your network configuration, considering this information:

- Each virtual switch can be connected to a physical adapter.
- Each virtual switch can be assigned one or more port groups.
- Virtual machines are connected to virtual switches using these port groups.



See the installation guide for deployment scenarios.

4 Gather necessary materials

Provide the required materials and verify that your management computer meets the requirements.

Required materials

You must provide these items:

- Management computer
- Monitor
- Keyboard
- Network cables

Management computer requirements

Make sure your management computer meets the minimum requirements.

Firewall Enterprise Admin Console	
Microsoft operating system	<ul style="list-style-type: none">• Windows Server 2008• Windows 7• Windows Vista• Windows XP Professional
Web browser	<ul style="list-style-type: none">• Microsoft Internet Explorer version 7 or later• Mozilla Firefox version 3.0 or later
Hardware	<ul style="list-style-type: none">• 2 GHz x86-compatible processor• 2 GB of system memory• 300 MB of available disk space• DVD drive• 1024 x 768 display• Network card• USB port

Control Center Client application	
Microsoft operating system	<ul style="list-style-type: none">• Windows Server 2008• Windows Server 2003• Windows XP Professional with SP2 or later• Windows Vista• Windows 7
Hardware	<ul style="list-style-type: none">• 3 GHz Intel Pentium 4 processor or higher• System memory• Windows Server or Windows XP: 3 GB (2 GB minimum)• Windows Vista or Windows 7: 4 GB (3 GB minimum)• 750 MB of available disk space• CD-ROM drive• 1024 x 768 display (1280 x 1024 recommended)• Network card• USB port• USB drive formatted in MS-DOS (configuration USB drive)

5 Set up your model S7032 appliance

Set up the appliance hardware.

- a Use the rack mount kit to install your appliance in a rack.
- b If you purchased optional network modules, install them in your appliance.

For instructions, see the hardware product guide for your appliance model.

- c Connect the appliance to a monitor and keyboard.
- d Connect the management network to the Ethernet port labeled *mgr1*.



Do not connect any other Ethernet ports at this time.

6 Set up ESXi management and virtual networks

Configure management settings on the appliance, install the VMware vSphere Client on your management computer, and configure virtual networks.

Change the default password

Change the default password for VMware ESXi.

- a Turn on the S7032 appliance.
- b When the status screen appears, press **F2**.
- c In the **Password** field, type `password`, then press **Enter**.
- d Change the password.



Passwords must be at least eight characters long.

Configure the management network

Perform these steps to configure the management network interface used by VMware ESXi.

- a On the status screen, select **Configure Management Network**, then press **Enter**.
- b Select the network adapter to use for the management network.
 - 1 Select **Network Adapters**, then press **Enter**.
 - 2 Make sure the network adapter that shows a status of **Connected** is selected, then press **Enter**.
- c Configure the following areas as appropriate for your management network:
 - VLAN
 - IP Configuration
 - IPv6 Configuration
 - DNS Configuration
- d When you are finished configuring the management network, apply the changes.
 - 1 Press **Esc** until the **Configure Management Network: Confirm** screen appears.
 - 2 Press **Y** to apply the changes.
 - 3 Press **Esc** to log off.

Install the VMware vSphere Client

Install the vSphere Client on your management computer.

- a Go to the URL shown on the S7032 appliance console. Click **Download VMware vSphere Client**.
- b Install the VMware vSphere Client, in the **Custom Setup** window of the installation wizard, select **Install VMware vSphere Update Service**.
- c Activate your VMware ESXi license.
For instructions, see the model S7032 installation guide.

Configure virtual networks

Configure virtual networking to prepare for the deployment of your firewalls.

For example virtual network configurations, see the model S7032 installation guide.

- a Start the VMware vSphere Client, then connect to the S7032 appliance.
- b Click the **Configuration | Networking | Add Networking**. The **Add Network Wizard** window appears.
- c Select **Virtual Machine | Next**. The **Network Access** window appears.
- d Select an existing vSwitch or create a new one to handle network traffic for this connection, then click **Next**.
 - To create a new vSwitch, select **Create a virtual switch**. Enable or disable physical Ethernet adapters for this vSwitch as needed.
 - To use an existing vSwitch, select it from the list.
- e Configure port group properties.
 - 1 In the **Network Label** field, type a name for this port group.
 - 2 [Optional] In the **VLAN ID** field, type a VLAN ID between 1–4095.
 - 3 Click **Next**.
- f Verify your changes, then click **Finish**.

Connect the virtual firewall to a network

Prior to configuration, each Firewall Enterprise, Virtual Appliance must be added to your virtual network.

- a In the VMware vSphere Client, select the virtual firewall.
- b From the **Inventory** menu, select **Virtual Machine | Edit settings**.
- c Connect the virtual firewall to a network.
 - 1 Select **Network Adapter 1**.
 - 2 Map the network adapter to the appropriate network connection.
 - 3 Make sure **Connect at power on** is selected, then click **OK**.
Repeat Step c for network adapters 2–10 as needed.

7 Install Firewall Enterprise management software

Install the Firewall Enterprise Admin Console and Control Center Client application on your management computer to connect to and manage firewalls.

Install the Firewall Enterprise Admin Console

Use the Admin Console in environments where you have a small number of firewalls to manage, or as a backup to Control Center.

- a Insert the firewall software DVD.
- b Run the Firewall Enterprise Admin Console setup.exe file.
- c Follow the on-screen instructions to complete the setup program.
McAfee recommends using the default settings.

Install the Control Center Client application

Use the Control Center Client application to connect to the Control Center Management Server.

- a Log on to the management computer as an administrator.
- b Insert the firewall software DVD.
- c Run the Firewall Enterprise Control Center Client application *CCnnnclientsetup.exe* file (where *nnn* is the version).
- d Follow the on-screen instructions.
 - 1 If another version of the Control Center Client application is already installed on this computer, decide if you want to overwrite the old version or install this new version at a different location. Make your selections and click **Next**.
 - 2 Accept the default settings when possible and click **Next** until the wizard is complete.

8 Configure each Firewall Enterprise, Virtual Appliance

You will need to determine which method to use to create your initial configuration. You can either utilize the Quick Start Program in the VMware Vsphere Client or you can use the Admin Console and the default factory settings.

Use the Quick Start Program

You can complete the initial configuration by accessing the command line in the VMware vSphere Client.

- a In the **Getting Started** tab, click **Power on this virtual machine** to start the Firewall Enterprise, Virtual Appliance.
- b Click the **Console** tab.

After startup is complete, the Quick Start Program appears.

- c Click anywhere inside the console window and press **Enter**.
- d Complete the Quick Start Program by entering the requested information.



Do not auto-register your virtual firewalls to the Control Center at this time.

Use the Admin Console default settings

Firewall Enterprise, Virtual Appliance includes default configuration settings that allow you to complete the configuration from the Admin Console.

- a In the **Getting Started** tab, click **Power on this virtual machine** to start the Firewall Enterprise, Virtual Appliance.



When the appliance does not find a configuration file and there is no response at the command line, the appliance loads the default settings.

- b If you want to designate the IP address and netmask of the internal interface, you must access the appliance through the console.
 - 1 Press **Enter** when the appliance searches for the configuration.
 - 2 Press **M** for minimal configuration and follow the prompts.
- c Connect the management computer to the network that is connected to the firewall internal network.
- d Start the Admin Console by selecting **Start | All Programs | McAfee | McAfee Firewall Enterprise v8 | Admin Console**.

Connect to the firewall internal IP address using these default settings:

- **Host name** — <MACaddress>_fwlocal.com
- **IP address** — 192.168.1.250 (internal) or the IP address you specified for a minimal configuration, 192.168.2.250 (external)
- **Username** — admin
- **Password** — admin



For complete information about all default settings, see the *McAfee Firewall Enterprise Product Guide*.

- e Follow the prompts to change your password.



Passwords must be at least eight alphanumeric characters long.

9 Configure the Control Center, Virtual Appliance and add firewalls


The Control Center, Virtual Appliance must be set up before firewalls can be managed.

Configure the Control Center, Virtual Appliance

Set up the Control Center, Virtual Appliance

- 1 In the VMware vSphere Client, select the Control Center.
- 2 From the **Inventory** menu, select **Virtual Machine | Edit settings**. The **Virtual Machine Properties** window appears.
- 3 Connect the Control Center to the appropriate network.
 - a Select **Network Adapter 1**.
 - b Map the network adapter to the appropriate network connection.
 - c Make sure **Connect at power on** is selected, then click **OK**.
- 4 Perform initial configuration.
 - a In the **Getting Started** tab, click **Power on this virtual machine** to start the Control Center.
 - b Click the **Console** tab. After startup is complete, a "Searching for configuration" message appears.
 - c Click anywhere inside the console window, then press **M**.
 - d Complete the initial configuration process by entering the requested information.

Add firewalls to the Control Center, Virtual Appliance

Enable SSH access for each firewall	<p>To add firewalls, the Control Center, Virtual Appliance must have SSH access to the firewall.</p> <ol style="list-style-type: none">1 Use the Firewall Enterprise Admin Console to connect to the firewall.2 Enable the SSH access control rule to allow the Control Center to connect to the firewall.
Add a firewall or HA cluster	<p>Perform these steps to add a new firewall or HA cluster to the Control Center, Virtual Appliance.</p> <ol style="list-style-type: none">1 In the Control Center Client application navigation bar, select Policy.  For option descriptions, press F1.2 Complete the wizard to add a firewall or cluster, then click Next.<ul style="list-style-type: none">• To add a standalone firewall, double-click the Firewalls node in the Policy tree.• To add a High Availability cluster, double-click the Clusters node in the Policy tree.3 Complete the information on the Firewall Connection Information page, then click Next.4 On the Firewall Registration Information page, select Register the firewall with this Management Server.5 Click Next.6 On the Summary page, verify the information, then click Register.7 After registration successfully completes, click Next.8 Retrieve items and categories from this firewall or cluster into Control Center, Virtual Appliance.<ol style="list-style-type: none">a On the Retrieval of the Firewall into Control Center page, select the items and categories to be retrieved.b Click Finish.9 Verify communication between the firewall or cluster and the Management Server.<ol style="list-style-type: none">a In the navigation bar, click Dashboards.b Click the Firewalls tab, and verify that a green light appears next to the firewall or cluster.

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

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