Upgrade Guide

McAfee Vulnerability Manager 3000 and 3100 Appliance Microsoft Windows Server 2008 R2

Issued 4/17/2012 15:21 / McAfee Vulnerability Manager 3000 and 3100 Appliance Microsoft Windows Server 2008 R2 Upgrade Guide
700-3712-00

Contents

Upgrading the McAfee Vulnerability Manager 3000 and 3100

This guide contains instructions on upgrading McAfee® Vulnerability Manager (MVM) 3000 and 3100 appliances to Microsoft Windows Server 2008 R2 (64-bit).

Overview

- Back up your existing Faultline database (only for the appliance running the database).
- Use the Backup/Restore utility to create a backup file of your appliance settings (like registry and engine ID).
- Upgrade the BIOS on the appliance.
- Upgrade the Windows operating system.
- Use the Backup/Restore utility to restore your appliance settings from your backup file.
- Install Microsoft SQL 2005 SP4 (only for the appliance running the database).
- Restore the Faultline database (only for the appliance running the database).
- Install the McAfee Vulnerability Manager components on the appliance.

Back up the SQL server database

Before performing an upgrade, use SQL Server Management Studio to create a backup of your McAfee Vulnerability Manager database so you can restore it after the upgrade.

1. Open SQL Server Management Studio: Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
2. Connect to the server by providing the proper authentication.
3. Expand the Databases in the Object Explorer.
4. Right-click the **Faultline** database and select **All Tasks | Backup Database**.

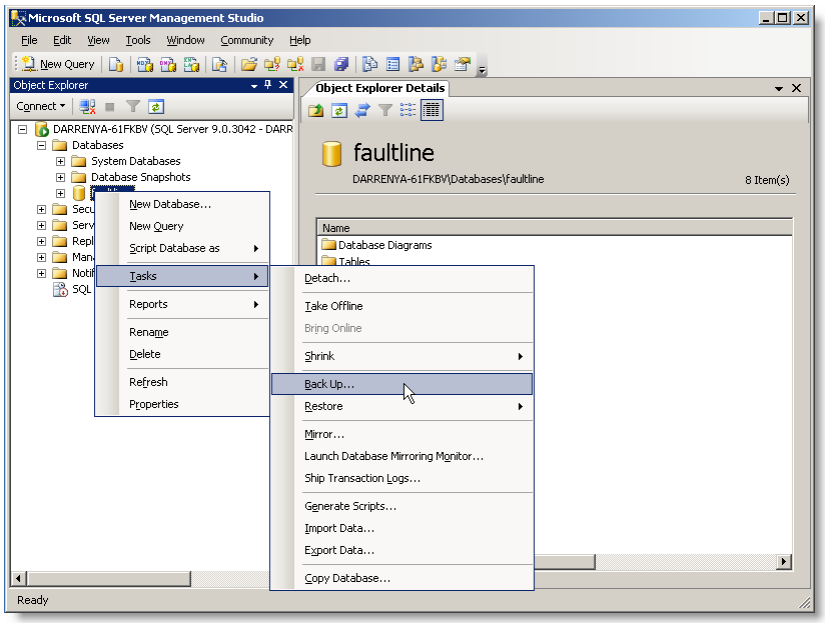

Figure 1: SQL Enterprise Manager – Getting to the Backup menu

5 In the **Back Up Database** dialog box, the backup destination is entered automatically. To add a different location, click **Add** to specify where to create the backup file.

6 (Optional) Select **Options | Verify Backup on finished** to have SQL make sure that the backup is correct.

7 Click **OK** to begin the backup process. A message appears when the backup is complete.

Back up the appliance settings

Use the Backup and Restore utility on the appliance to save your configuration settings to a file. Back up your settings before you upgrade the operating system on your appliance.

The utility only saves configuration settings for the appliance it is run on. You must run this utility on each McAfee Vulnerability Manager appliance that you want to restore from a backup file.

For MVM 3000 users – The backup wizard is on the Software Setup disc and the BIOS upgrade is provided on a USB storage device. You can save your appliance settings file to the USB storage device or a network folder.

For MVM 3100 users – The backup wizard and BIOS upgrade files are on the Software Setup disc. You can save your appliance settings file to a network folder. If you want to save the file to a USB storage device, you must provide your own storage device.

Caution: When upgrading to Microsoft Windows 2008 R2, all files on the local hard drive are deleted. Save your backup file to a network folder or a USB device.

1. Insert the Software Setup disc, view the contents of the disc, then double-click **MVM_Autorun.exe**.
2. On the Welcome screen, click **Next**.
3. Select **Yes** to create an appliance backup file, then click **Next**.
4. Browse to and select a file location, type a name for the file, then click **Save**.
5. Click **Next**.
6. Type a password for the backup file, then click **Next**. The password must be at least 8 characters and consist of letters and numbers.
7. (Optional) Select **View Database Backup Instructions** to view instructions on how to backup your McAfee Vulnerability Manager database. This is available only when the database is installed on the appliance.
8. Click **Apply**.
9. When the backup is complete, click **Close**.

Upgrade the BIOS on the MVM3000

The USB storage device provides a BIOS upgrade for your MVM3000 appliance. An older BIOS doesn't activate Windows Server 2008 R2 (64-bit) during installation. You must activate it manually.

If you have an MVM3100 appliance, you must use the Software Setup disc and follow the procedure *Upgrade the BIOS on the MVM3100* (page 8).

Caution: If you don't upgrade the BIOS on your appliance, you might need to manually activate Windows Server 2008 R2 manually.

1. When the appliance settings backup file is complete, restart your appliance with the USB device inserted.
2. As the system boots, press **F11** to initiate the boot menu.
3. Type the password, then press **Enter**. The default password is F0UNDP41 (F-zero-UNDP-four-one).
4. Select **Hard Drive C:**, select the USB device, then press **Enter**. Review the BIOS upgrade instructions.
5. Press any key to continue.
6. Review the disclaimer, then press **Y** to accept. The appliance restarts.
7. As the system boots, press **F11** to initiate the boot menu.
8. Type the password, then press **Enter**.
9. Select **Hard Drive C:**, select the USB device, then press **Enter**.
10. When the BIOS upgrade is complete, press any key to restart the appliance.

Upgrade the BIOS on the MVM3100

The Software Setup disc provides a BIOS upgrade for your MVM3100 appliance. An older BIOS doesn't activate Windows Server 2008 R2 (64-bit) during installation. You must activate it manually.

If you have an MVM3000 appliance, you must use the USB device and follow the procedure *Upgrade the BIOS on the MVM3000* (page 7).

Caution: If you don't upgrade the BIOS on your appliance, you might need to activate Windows Server 2008 R2 manually.

1. When the appliance settings backup file is complete, the BIOS upgrade wizard appears. Click **Yes** to continue.
2. To upgrade the BIOS, click **Yes**.
3. When the BIOS upgrade is complete, click **OK**.
4. Click **OK** to close the wizard.
5. Restart your appliance to apply the new BIOS.

Upgrade the operating system

The upgrade kit contains a Recovery Image disc with a Windows Server 2008 R2 image for the McAfee Vulnerability Manager appliance. There are separate Recovery Image discs for the MVM 3000 and the MVM 3100.

If your appliance is running an older BIOS, you must upgrade the BIOS before imaging with the new operating system.

1. Insert the Recovery Image disc, then restart the appliance.
2. The reimaging process autoruns. The reimaging process could take 30 minutes to complete.
3. When reimaging is complete, remove the Restore DVD disc.
4. Click **Exit** to restart your appliance.
5. When prompted, type a password for the appliance administrator (applianceadmin), then press **Enter**. The appliance restarts.
6. Log in with the appliance administrator password. The operating system applies the user settings.

Reinstall McAfee Vulnerability Manager software

After upgrading the operating system on your appliance and installing the necessary software, you must install McAfee Vulnerability Manager on your appliance using the Software Setup disc.

If you stored your backup file on a network folder, you must enable some services so the appliance can access your network. See *Enable services to access a network folder* (page 11).

Refer to the *McAfee Vulnerability Manager Installation Guide* for details about installing the product.

1. Insert the Software Setup disc.
2. On the Welcome screen, click **Next**.
3. Select **Yes**, then click **Next**.
4. Read the restore operation information, then click **Next**.
5. Browse to and select the backup file for the appliance, click **Open**, then click **Next**.
6. Type the password for your backup file, then click **Next**.
7. Select **Yes** to restore the host name.

   Caution: If you choose not to restore the host name, some of the product components might not work properly with your appliance.
8. Click **Next**.
9. Click **Reboot System**, then click **Apply**.
10. Click **Next**. Optionally, click on the quick start guide link for more information about installing and using the product.
11. Select the McAfee Vulnerability Manager version and the SQL Server version you want to install on this appliance, then click **Next**. If you aren't installing the product database, then don't select a SQL Server version.
12. Type the password and the SQL Server product key, then click **Next**. McAfee recommends using the sa login and password. Optionally, select **Prompt Database Restore** before installing the product to view instructions on how to restore the product database after Microsoft SQL Server is installed.
13. Click **Apply**. SQL Server and the service pack are installed.
14. Restore your Faultline database (see *Restore the McAfee Vulnerability Manager database* (page 9)). If you selected the message prompt, click **Close** to exit the instructions.
15. Click **Apply** to close the restore wizard.
16. When the product installation wizard starts, select the components you want to install on the appliance. When the product is installed and the appliance restarts, the Network Security Wizard starts automatically. See *McAfee Vulnerability Manager Network Security Wizard* (page 14).

    Note: For product and content updates, if the appliance running FSUpdate is not running SQL Server, then you must install the SQL Client Tools and SQL Server Management Objects for FSUpdate to function properly. If the appliance running FSUpdate is running SQL Server, then you must install the SQL Management Objects. See *Install Microsoft SQL Client Tools* (page 12) and *Install Microsoft SQL Server Management Objects* (page 13).

Restore the McAfee Vulnerability Manager database

After you reinstall the McAfee Vulnerability Manager software, you need to restore the database from a backup.

1. Using the configuration manager, stop all scan engines. Open the configuration manager, expand the product system tree in the left pane, select a scan engine, and click **Stop**. You must do this for each scan engine.
2. Select **Start** | **All Programs** | **Microsoft SQL Server** | **SQL Server Management Studio**.
3. Log on to SQL Server Management Studio.
4. Right-click **Databases**, then select **Restore Database**.
   - Type `Faultline` in the **To database** field.
   - Select **From device**, then click **Select Devices**.

Note: With McAfee Vulnerability Manager 6.5 and later, you don't have to use Faultline as the database name. See McAfee Vulnerability Manager database name (page 12) for more information.

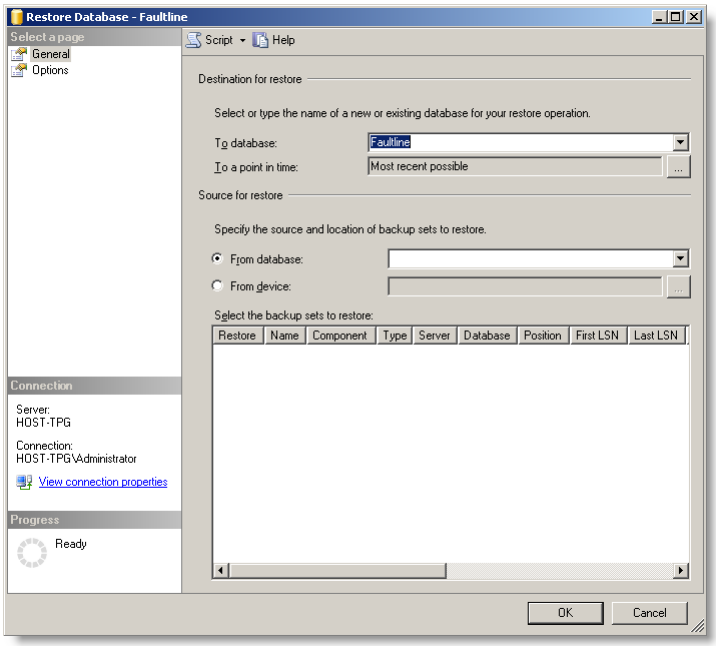

Figure 2: SQL Server Back up

5 In the **Choose Restore Devices** dialog box, click **Add**.
- Type file name and location of the backup files are located, then click **OK** twice.

6 (Optional) On the **Options** tab, you can edit the rows in the *Move to physical file name* column to specify the location and names of the physical files of the restored McAfee Vulnerability Manager database.

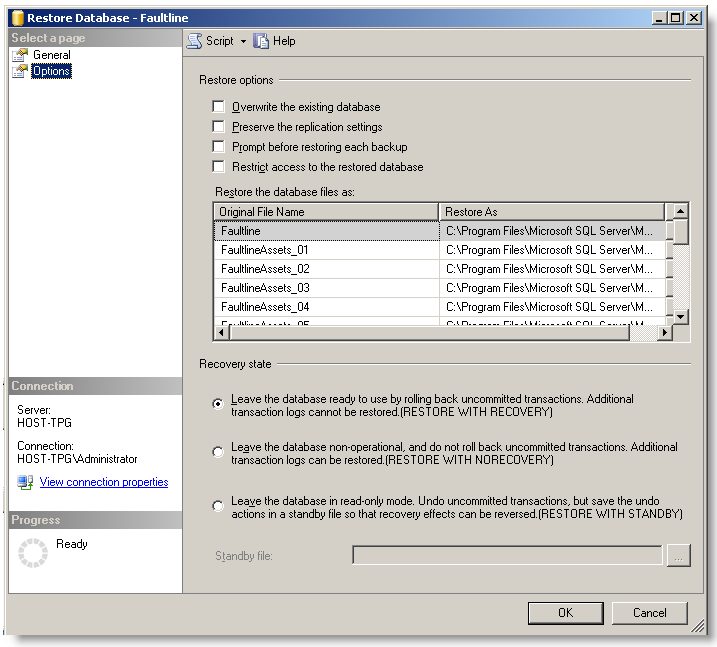

Figure 3: Restore database

7 Click **OK**, to begin restoring the database. When the process is complete, click **OK**.

8 From the *Object Explorer*, expand **Security**, right-click **Logins**, then select **New Login**.
- Type `faultline` for the **Login** name.
- Select **SQL Server authentication**, then type the faultline user password.
- Deselect **Enforce password policy**, then click **OK**.

9 Expand **Databases**, select **faultline**, then click **New Query**.

10 Type `exec sp_change_users_login 'Update_One', 'faultline', 'Faultline'`, then click **Execute**. This associates the faultline user login with the faultline database.

Enable services to access a network folder

If you saved your backup files to a network folder, you must enable some services so the appliance can access your network.

1 Select **Start | Administrative Tools | Services**.

2 Right-click **Server**, then select **Properties**.

3 Select **Manual** for the Startup type, then click **Apply**.

4 Click **Start**, then click **OK**.

5 Right-click **Computer Browser**, then select **Properties**.

6 Select **Manual** for the Startup type, then click **Apply**.

7 Click **Start**, then click **OK**.

8 Close the Services window.

McAfee Vulnerability Manager database name

With McAfee Vulnerability Manager 6.5 and later, you don't have to use Faultline as the McAfee Vulnerability Manager database name.

If you use a database name other than Faultline, you must add a string to the `HKEY_LOCAL_MACHINE\SOFTWARE\Foundstone\Foundscan` registry key for Microsoft Windows 2003 or `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Foundstone\Foundscan` registry key for Microsoft Windows 2008 R2. The string must be `DBName` with the value of the name created for the McAfee Vulnerability Manager database.

If you use a database name other than Faultline, you should add the DBName registry key to any system that runs one or more of the following McAfee Vulnerability Manager applications or services:

- Scan controller
- API server
- Report engine
- Notification service
- Data synchronization service
- Configuration manager

Install SQL Client Tools

If you run FSUpdate using a scan controller that is not installed with the database, you must install SQL Client Tools and the SQL Server Management Objects (SMO) for FSUpdate to function properly.

If you use an All-in-One configuration, or you run FSUpdate from a scan controller that is installed with the database, you only need to install the SQL Server Management Objects.

Caution: Install the SQL Client Tools after you install McAfee Vulnerability Manager.

1. Double-click **SqlncIi_x64.msi**. This file is on the Software Setup disc. The default location is E:\SQL2005\Client Tools.
2. Click **Next**.
3. Select **I accept the licensing terms and conditions**, then click **Next**.
4. Click **Next**.
5. Type your registration information, then click **Next**.
6. For Client Components, select **This feature, and all subfeatures, will be installed on local hard drive**, then click **Next**.
7. Click **Next**.
8. Click **Install**.
9. Select **I want to complete this action** on the UAC notification.
10. Click **Finish**.
11. Copy **bcp.exe** and **bcp.rll** to `D:\Foundstone`. These files are on the Software Setup disc. The default location is `E:\SQL2005\Client Tools`.

Install SQL Server Management Objects (SMO)

If you run FSUpdate using a scan controller that is not installed with the database, you must first install SQL Client Tools, then install the SQL Server Management Objects (SMO) for FSUpdate to function properly.

If you use an All-in-One configuration, or you run FSUpdate from a scan controller that is installed with the database, you only need to install the SQL Server Management Objects.

Caution: Install the SQL Server Management Objects after you install McAfee Vulnerability Manager.

1. Double-click **SQLServer2005_XMO_x64.msi**. This file is on the Software Setup disc. The default location is E:\SQL2005\Client Tools.
2. Click **Next**.
3. Select **I accept the licensing terms and conditions**, then click **Next**.
4. Type in your registration information, then click **Next**.
5. Click **Install**.
6. Select **I want to complete this action** on the UAC notification.
7. Click **Finish**.

Network Security Wizard

The McAfee Vulnerability Manager Network Security Wizard helps you make changes to the network security configuration on this system. The Network Security Wizard provides a Simple and Advanced setup.

- **Simple** – Opens the ports required for any installed product services on the server, and close unused ports.
- **Advanced** – Adjusts the system firewall settings, changes service communication ports, and adds additional rules for your network security settings.

Simple setup

Use the Simple setup to open only the required ports for any installed product services on the server.

When the product installation is complete and the system restarts, the Network Security Wizard appears.

1. Select **I want to complete this action** on the UAC notification.
2. On the Welcome screen, click **Next**.
3. Select the Windows Advanced Firewall profiles, ICMP Echo Requests, and Edge Traversal options.
   - **Windows Advanced Firewall profiles** – Select the firewall profiles (Domain, Public, Private) that should be modified by the Network Security wizard.
   - **Allow ICMP Echo Requests** – Select this option to allow the appliance to respond to ICMP echo requests (ping).
   - **Enable Edge Traversal** – Select this option to make sure that inbound tunneled traffic is passed through the firewall. If devices in your McAfee Vulnerability Manager environment tunnel traffic, select this checkbox.
4. Select **Simple**, then click **Next**.
5. Click **Apply**.

Note: McAfee recommends running McAfee Vulnerability Manager Update after upgrading to make sure you have the latest product updates.

Advanced setup

Use the Advanced setup to adjust the system firewall settings, change service communication ports, and add additional rules for your network security settings.

When the product installation is complete and the system restarts, the Network Security Wizard appears. The following steps depend on which McAfee Vulnerability Manager components are installed on this system.

Caution: If you leave an IP address field blank, the service is open to any host on the network.

1. Select **I want to complete this action** on the UAC notification.
2. On the Welcome screen, click **Next**.
3. Select the Windows Advanced Firewall profiles, ICMP Echo Requests, and Edge Traversal options.
   - **Windows Advanced Firewall profiles** – Select the firewall profiles (Domain, Public, Private) that should be modified by the Network Security wizard.
   - **Allow ICMP Echo Requests** – Select this option to allow the appliance to respond to ICMP echo requests (ping).
   - **Enable Edge Traversal** – Select this option to make sure that inbound tunneled traffic is passed through the firewall. If devices in your McAfee Vulnerability Manager environment tunnel traffic, select this checkbox.
4. Select **Advanced**, then click **Next**.
5. If the database is installed, select **Database Firewall** options, then click **Next**. The Database Firewall allows you to specify host IP address ranges that are permitted to access the database.
   - **Allow access to the database server** – Allow other systems access to the database.
   - **Allow all hosts** – Allow all hosts access to the database.
   - **Allow only these hosts** – Allow only the IP addresses specified access to the database. If you select this option, type in the IP addresses or address ranges.
   - **SQL Server Port** – Type in a port number if you configured SQL Server to operate on a non-standard port.
6. If an API server is installed, select **API Server Firewall** options, then click **Next**. The API Server Firewall allows you to specify host IP address ranges that are permitted to access the API server.
   - **Allow access to the API Server** – Allow other systems access to the API server.
   - **Allow all hosts** – Allow all hosts access to the API server.
   - **Allow only these hosts** – Allow only the IP addresses specified access to the API server. Type in the IP addresses or address ranges.
   - **Override Default Port** – Change the API server service port. Type in a port number.
7. If the configuration manager is installed, select **Configuration Manager Firewall** options, then click **Next**. The Configuration Manager Firewall allows you to specify host IP address ranges that are permitted to access the configuration manager.
   - **Allow access to the Configuration Manager** – Allow other systems access to the configuration manager.
   - **Allow all hosts** – Allow all hosts access to the configuration manager.
   - **Allow only these hosts** – Allow only the IP addresses specified access to the configuration manager. Type in the IP addresses or address ranges.
   - **FCM Server Port** – Use the configuration manager console to change the FCM Server Port, then re-run the Network Security Wizard.
8. If the report engine is installed, select **Report Server Firewall** options, then click **Next**. The Report Server Firewall allows you to specify which hosts can send report requests to the report engine.
   - **Allow access to the Report Server** – Allow other systems to send report requests to the report engine.
   - **Allow all hosts** – Allow all hosts to send report requests to the report engine.
   - **Allow only these hosts** – Allow only the IP addresses specified to send report requests to the report engine. Type in the IP addresses or address ranges.
   - **Override Default Port** – Change the report server port. Type in a port number.
9. If a scan controller is installed, select **Scan Controller Firewall** options, then click **Next**. The Scan Controller Firewall allows you to specify host IP address ranges that are permitted to access the scan controller.
   - **Allow access to the Scan Controller** – Allow other systems access to the scan controller.
   - **Allow all hosts** – Allow all hosts access to the scan controller.
   - **Allow only these hosts** – Allow only the IP addresses specified access to the scan controller. Type in the IP addresses or address ranges.
   - **Override Default Port** – Change the scan controller service port. Type in a port number.

10 If the enterprise manager is installed, select the **Enterprise Manager Firewall** option, then click **Next**.

- Select **Yes** to specify IP address ranges, then type the IP address ranges permitted to access the enterprise manager.
- Select **No** to allow any IP address to access the enterprise manager.

11 If the McAfee Vulnerability Manager Notification Service is installed, select **Notification SNMP Rules** options, then click **Next**. The Notification SNMP Rules allows you to accept inbound SNMP messages.

- **Allow SNMP access to the Notification Service** – Accept inbound SNMP messages to the McAfee Vulnerability Manager Notification Service.
- **Allow all hosts** – Allow the McAfee Vulnerability Manager Notification Service to accept inbound SNMP messages from all hosts.
- **Allow only these hosts** – Allow the McAfee Vulnerability Manager Notification Service to only accept inbound SNMP messages from the IP addresses specified. Type in the IP addresses or address ranges.
- **SNMP Server Port** – Type in a UDP port number if your SNMP service listens on a non-default port.

Note: If McAfee Vulnerability Manager Notification Service is installed but inbound SNMP isn't configured, a message appears stating that the firewall doesn't accept inbound SNMP messages. If allowing inbound SNMP messages is required, configure the SNMP settings in the Enterprise Manager (as Global Administrator) and run this wizard again to configure the firewall.

12 Select the **Remote Desktop Firewall** options, then click **Next**.

- **Enable Remote Desktop service** – Enable the remote desktop service on this system.
- **Allow all hosts** – Allow all hosts remote access to this system.
- **Allow only these hosts** – Allow only the IP addresses specified remote access to this system. Type in the IP addresses or address ranges.
- **Override Default Port** – Change the remote desktop service port. Type in a port number.

13 Create additional firewall rules, then click **Next**. When you add or edit a firewall rule, you must click **OK** to save your settings.

- **Add** – Add a custom firewall rule.
- **Edit** – Edit the selected firewall rule.
- **Delete** – Delete the selected firewall rule.

The following options are available when you create or edit a firewall rule.

- **Service Name** – Type the name of the service.
- **Protocol** – Select the TCP or UDP protocol.
- **Service Port** – Type the port number used by the service.
- **Allow access to the service** – Open this service to other hosts.
- **Allow all hosts** – Allow all hosts access to this service.

- **Allow only these hosts** – Allow only the IP addresses specified access to this service. Type in the IP addresses or address ranges.

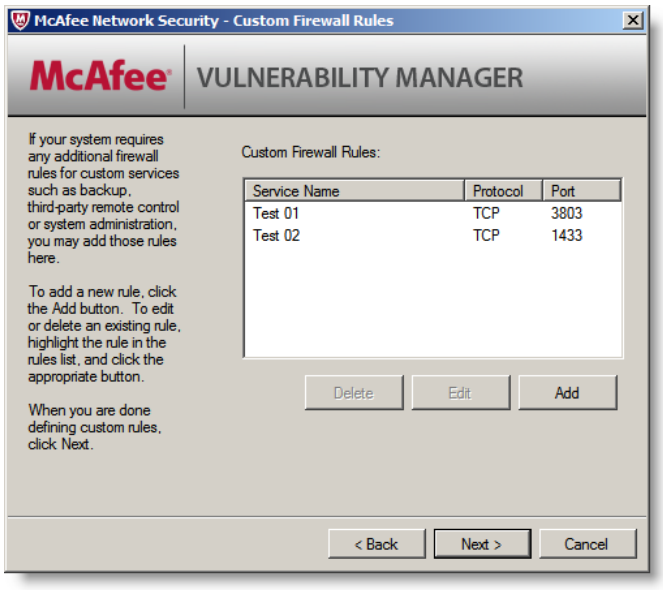

Figure 4: Custom firewall rules

14 On the Confirm Settings screen, click **Apply** to confirm the firewall settings.

15 On the Firewall Configuration Complete screen, click **Finish** to restart the system.

Note: If you selected Advanced and then accepted the default settings, the Network Security Wizard doesn't prompt you to restart the appliance. If this happens, restart the appliance. Some changes don't take effect until after the system is restarted.

16 Log on with the administrator account name and password you created in the previous steps.

Note: McAfee recommends running McAfee Vulnerability Manager Update after upgrading to make sure you have the latest product updates.

Run the product agent as an administrator

After upgrading to Windows Server 2008 R2, the Foundstone Configuration Agent might not appear in the system tray.

The Microsoft user account control (UAC) may prevent the agent from running. To resolve this issue, set the FCAgentSettings.exe file to run as an administrator. This should be done on all systems running McAfee Vulnerability Manager, except for the system running the configuration manager.

1. Open the product FCM folder. For appliances, this should be D:\Program Files (x86)\Foundstone\FCM.
2. Right-click **FCAgentSettings.exe**, then select **Properties**.
3. Click **Compatibility**, select **Run this program as an administrator**, then click **OK**.
4. Double-click **FCAgentSettings.exe** to start the configuration agent, if necessary. You might need to start the agent.