



CHAPTER 14

McAfee Foundstone

To configure MARS to pull data from McAfee Foundstone (formerly known as Foundstone FoundScan), you must perform three tasks:

1. Configure McAfee Foundstone to enable data retrieval by MARS.
2. Add the McAfee Foundstone server to MARS using the web interface.
3. Schedule the interval at which the McAfee Foundstone server data is pulled by MARS.

This chapter contains the following topics:

- [Enable McAfee Foundstone 5.x and later to Use TCP/IP, page 14-1](#)
- [Enable McAfee Foundstone \(versions prior to 5.0\) to Use TCP/IP, page 14-2](#)
- [Add and Configure a McAfee Foundstone Device in MARS, page 14-3](#)

Enable McAfee Foundstone 5.x and later to Use TCP/IP

To enable TCP/IP on Foundstone 5.0 and 6.0, use the SQL Server Configuration Manager. As part of this configuration, you must disable the secure communications.

To enable the TCP/IP network protocol, perform the following steps:

Step 1 On the **Start** menu, choose **All Programs**, point to **Microsoft SQL Server** and then click **SQL Server Configuration Manager**.



Tip Optionally, you can open Computer Manager by right-clicking **My Computer** and choosing **Manage**. In Computer Management, expand **Services and Applications**, expand **SQL Server Configuration Manager**.

Step 2 Expand **SQL Server Network Configuration**, and then click **Protocols for InstanceName**.

Step 3 In the list of protocols, right-click the **TCP/IP** protocol, and then click **Enable**.

The icon for the protocol changes to show that the protocol is enabled.

Step 4 In the right pane, enable the IP address of the Local Controller that is monitoring this Foundstone server.

Step 5 Click **Apply**.

Step 6 Right-click on **Protocols for InstanceName**, and select **Properties**.

Step 7 In the Force Protocol Encryption box, verify the **OFF** option is selected.

This option disables secure communications between the MARS appliance and the Foundstone Server.

Step 8 Click **OK** to close Properties.

Step 9 Click **OK** to close SQL Server Configuration Manager.

Enable McAfee Foundstone (versions prior to 5.0) to Use TCP/IP



Note

This procedure is only required for Foundstone versions prior to 5.0.

To configure McAfee Foundstone to provide data to MARS, follow these steps:

Step 1 Run command **svrnetcn** at the DOS prompt on the host where McAfee Foundstone is installed.

```

C:\WINNT\system32\cmd.exe
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>svrnetcn
'svrnetcn' is not recognized as an internal or external command,
operable program or batch file.

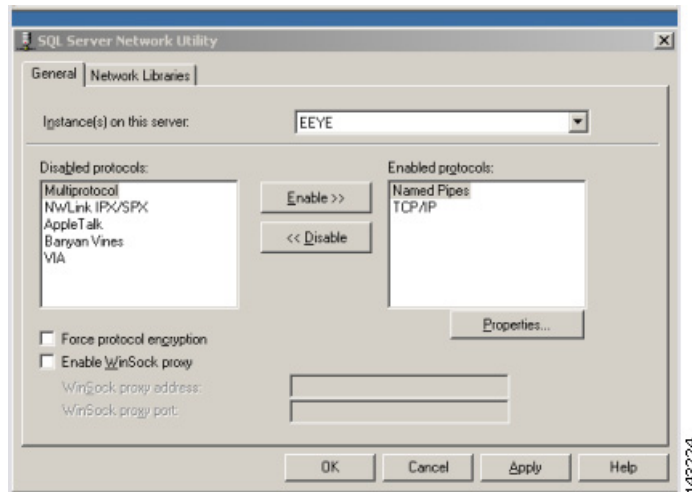
C:\Documents and Settings\Administrator>svrnetcn

C:\Documents and Settings\Administrator>cd \

C:\>
C:\>
C:\>
C:\>svrnetcn

C:\>_
  
```

Step 2 In the SQL Server Network Utility dialog box, enable TCP/IP by moving **TCP/IP** from the Disabled Protocols list to Enabled Protocols list.



- Step 3** Verify that the **Force protocol encryption** checkbox is cleared.
- Step 4** Click **Apply**.
- Step 5** Click **OK** to close SQL Server Network Utility.

Add and Configure a McAfee Foundstone Device in MARS

To add a McAfee Foundstone device in MARS, follow these steps:

- Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.
- Step 2** Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.
- Step 3** Enter the device name and IP addresses if adding a new host.
- Step 4** Click **Apply**.
- Step 5** Click the **Reporting Application** tab.
- Step 6** From the Select Application list, select **McAfee Foundstone ANY**.
- Step 7** Click **Add**.

→ *Database Name:

→ *Access Port:

→ *Access Type:

Login:

Password:

143215

Step 8 Enter the following information:

- **Database Name**—The name for this database.
- **Access Port**—The default access port is 1433.
- **Access Type**—Verify the value is MS SQL.
- **Login**—The login information for the database.
- **Password**—The password for the database.

Step 9 Click **Submit**.

Step 10 Click **Apply**.

Once you activate this device (click **Activate** in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see [Scheduling Topology Updates](#), page 1-18.
