Getting Started

User interface components

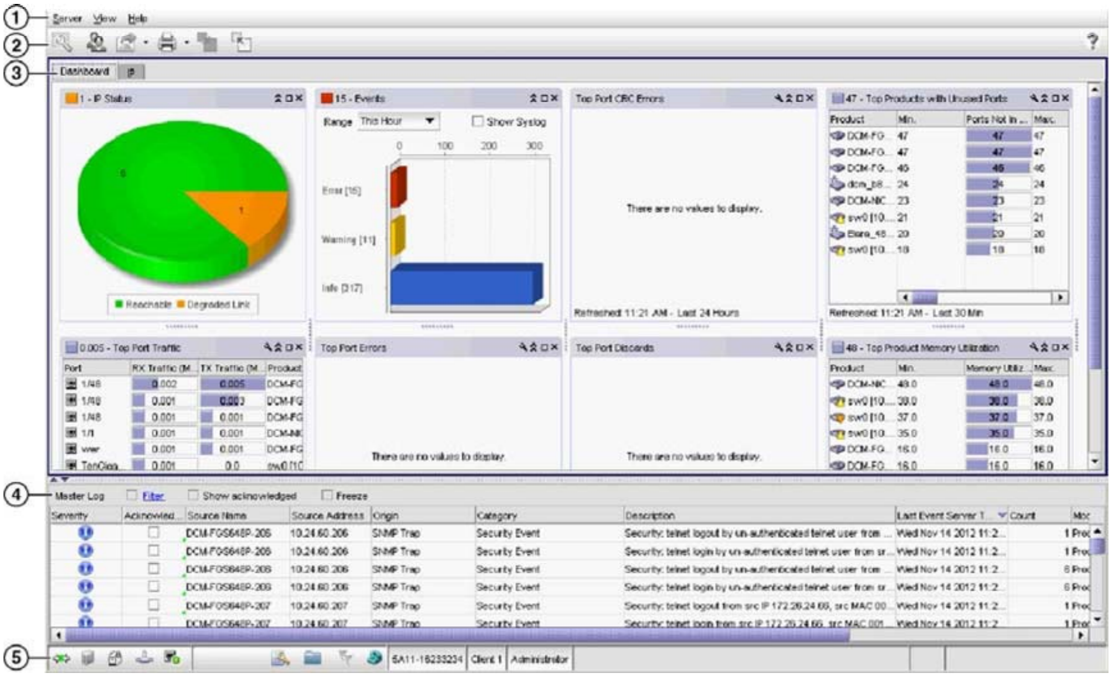
NOTE
The Management application does not support I18N internationalization and localization.

The Management application provides easy, centralized management of the network, as well as quick access to all product configuration applications. Using this application, you can configure, manage, and monitor your networks with ease.

The Management application's main window contains a number of areas. The following figures illustrate the various areas, and descriptions of the areas follow the figures.

NOTE
Some widgets may be hidden. To display a widget to the **Dashboard** tab, click the Customize Dashboard icon ("Customizing the dashboard widgets and monitors" on page 223).

FIGURE 1 Main window



There are no values to display.

Refreshed 11:21 AM - Last 24 Hours

Product	Min.	Ports Not In ...	Max.
DCM-FG...	47	47	47
DCM-FG...	47	47	47
DCM-FG...	46	46	46
dcm_b8...	24	24	24
DCM-NC...	23	23	23
sw0 [10....	21	21	21
Elara_48...	20	20	20
sw0 [10....	18	18	18

Refreshed 11:21 AM - Last 30 Min

Port	RX Traffic (M...	TX Traffic (M...	Product
1/48	0.002	0.005	DCM-FG
1/48	0.001	0.003	DCM-FG
1/48	0.001	0.001	DCM-FG
1/1	0.001	0.001	DCM-NI
vwr	0.001	0.001	DCM-FG
TenGig...	0.001	0.0	sw0 [10

There are no values to display.

There are no values to display.

Product	Min.	Memory Utiliz...	Max.
DCM-NC...	48.0	48.0	48.0
sw0 [10....	38.0	38.0	38.0
sw0 [10....	37.0	37.0	37.0
sw0 [10....	35.0	35.0	35.0
DCM-FG...	16.0	16.0	16.0
DCM-FG...	16.0	16.0	16.0

Severity	Acknowled...	Source Name	Source Address	Origin	Category	Description	Last Event Server T...	Count	Mod
●	□	DCM-FGS648P-206	10.24.60.206	SNMP Trap	Security Event	Security: telnet logout by un-authenticated telnet user from ...	Wed Nov 14 2012 11:2...	1	Proc
●	□	DCM-FGS648P-206	10.24.60.206	SNMP Trap	Security Event	Security: telnet login by un-authenticated telnet user from sr...	Wed Nov 14 2012 11:2...	1	Proc
●	□	DCM-FGS648P-206	10.24.60.206	SNMP Trap	Security Event	Security: telnet logout by un-authenticated telnet user from ...	Wed Nov 14 2012 11:2...	6	Proc
●	□	DCM-FGS648P-206	10.24.60.206	SNMP Trap	Security Event	Security: telnet login by un-authenticated telnet user from sr...	Wed Nov 14 2012 11:2...	6	Proc
●	□	DCM-FGS648P-207	10.24.60.207	SNMP Trap	Security Event	Security: telnet logout from src IP 172.26.24.66, src MAC 00...	Wed Nov 14 2012 11:2...	1	Proc
●	□	DCM-FGS648P-207	10.24.60.207	SNMP Trap	Security Event	Security: telnet login from src IP 172.26.24.66, src MAC 001...	Wed Nov 14 2012 11:2...	1	Proc

1. **Menu bar —** Lists commands you can perform on the Management application. The available commands vary depending on which tab (IP or Dashboard) you select. For a list of available commands, refer to "Application Menus".
2. **Toolbar —** Provides buttons that enable quick access to dialog boxes and functions. The available buttons vary depending on which tab (IP or Dashboard) you select. For a list of available commands, refer to "IP main toolbar" on page 299 or "Dashboard toolbar" on page 217.
3. **Tabs** — Provides quick access to the following views:
   - **Dashboard tab —** Provides a high-level overview of the network managed by Management application server. For more information, refer to "Dashboard Management" on page 215.
   - **IP tab —** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the "IP tab overview".
4. **Master Log** — Displays the Master Log.
5. **Status bar —** Displays the connection, port, product, special event, Call Home, and backup status, as well as Server and User data.

Management server and client

The Management application has two parts: the server and the client. The server is installed on one machine and stores device-related information; it does not have a user interface. To view information through a user interface, you must log in to the server through a client. The server and clients may reside on the same machine, or on separate machines. If you are running Professional, the server and the client must be on the same machine.

Logging in to a server from the server machine

You must log in to a server to monitor your network.

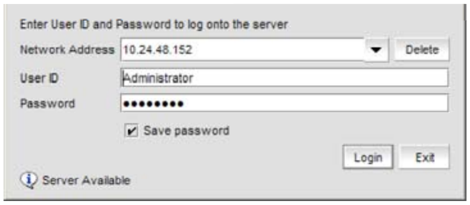
NOTE
You must have an established user account on the server to log in.

To log in to a server, complete the following steps.

1. From the server machine, double-click the desktop icon or open the application from the **Start** menu.

   The **Log In** dialog box displays (Figure 2).

FIGURE 2 Log In dialog box



Enter User ID and Password to log onto the server

Network Address 10.24.48.152

User ID Administrator

Password ••••••••

☑ Save password

Server Available

2.Remove a server from the **Network Address** list by selecting the IP address and clicking **Delete**.

3. Choose one of the following options:
   - If you configured authentication to CAC, enter your PIN in the CAC PIN field.
   - If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+), or a switch, complete the following steps.

   a. Enter your user name and password.
      The defaults are **Administrator** and **password**, respectively.

      NOTE
      Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.

   b. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
      To change your password, refer to "Changing your password" on page 195.

4. Click **Login**.
5. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Launching a remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache. To clear the previous version, refer to "Clearing previous versions of the remote client" on page 4.

The remote client requires Oracle JRE. For the current supported JRE version for the Management application, refer to the Release Notes. For the website listing patch information, go to *http://www.oracle.com/technetwork/java/javase/downloads/index.html*.

NOTE
For higher performance, use a 64-bit JRE.

NOTE
If you are managing more than 9000 SAN ports or 200 IP devices, the client is not supported on 32-bit systems.

To launch a remote client, complete the following steps.

1. Choose one of the following options:
   - Open a web browser and enter the IP address of the Management application server in the **Address** bar.

     If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Port_Number*.

     If this is the first time you are accessing this version of the Management application, this creates a start menu shortcut automatically in the Management application program directory.

     For Linux systems, remote client shortcuts are not created.
   - Select *Management_Application* (*Server_IP_Address*) in the Management application program directory from the start menu.

   The web client login page displays.

2. Click **Desktop Client**.

   The Management application web start page displays.

3. Click the **Web Start the Client** link.

   The **Log In** dialog box displays.

4.Log in to another server by entering the IP address to the other server in the **Network Address** field.

NOTE
The server must be the exact same version, edition, starting port number, and network size as the client.

5.Remove a server from the **Network Address** list by selected the IP address and clicking **Delete**.

6. Choose one of the following options:

- If you configured authentication to CAC, enter your PIN in the CAC PIN field.
- If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+), or a switch, complete the following steps.

    a. Enter your user name and password.
    The defaults are **Administrator** and **password**, respectively.

    NOTE
    Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.

    b. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
    To change your password, refer to "Changing your password" on page 195.

7. Click **Login**.

8. Click **OK** on the **Login Banner** dialog box.

    The Management application displays.

Clearing previous versions of the remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache.

To clear the Java cache, complete the following steps.

1. Select **Start > Settings > Control Panel > Java**.

    The **Java Control Panel** dialog box displays.

2. Click **View** on the **General** tab.

    The **Java Cache Viewer** dialog box displays.

3. Right-click the application and select **Delete**.

4. Click **Close** on the **Java Cache Viewer** dialog box.

5. Click **OK** on the **Java Control Panel** dialog box.

    To create a remote client link in the **Start** menu, refer to "Launching a remote client" on page 3.

Logging in to the web client

You must log in to a Management application server to monitor the network. To launch a web client, complete the following steps.

1. Choose one of the following options:

    - Open a web browser and enter the IP address of the Management application server in the **Address** bar.

If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address:Port_Number*.

If this is the first time you are accessing this version of the Management application, this creates a start menu shortcut automatically in the Management application program directory.

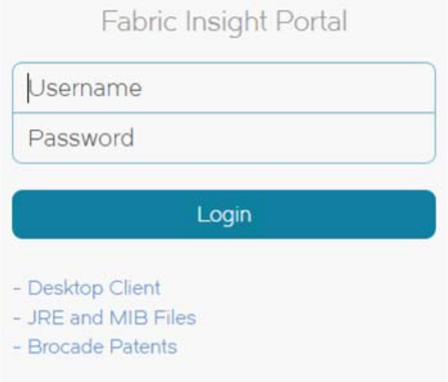
For Linux systems, remote client shortcuts are not created.

- Select *Management_Application* (*Server_IP_Address*) in the Management application program directory from the start menu.

The web client login page displays.

The web client login page displays with the server name and IP address in the upper left. You can launch the Java client from any page of the web client by clicking **Desktop Client**. You can download the client bundle (64-bit OS only), JRE, or MIB files by clicking **JRE and MIB files**.

FIGURE 3 Management application web client log in page



2. Enter your user name and password.

   NOTE
   Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.

3. Press **Enter** or click the login arrow icon.
4. Click **OK** on the **Login Banner**.

   The Management application web client displays.

   NOTE
   If the Administrator disconnects the web client using the **Active Sessions** dialog box (**Server > Active Sessions**), the web client redirects to the login page after three minutes or as soon as you make a selection.

Launching the Configuration Wizard

You can re-launch the Configuration wizard to change the following configurations:

- Server IP
- Server Ports

NOTE
Changes to these configurations require a server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **14.2.1 > Server Management Console**).

1. Choose one of the following options:
   - On Windows systems, select **Start > Programs >** *Management_Application_Name* **14.2.1>** *Management_Application_Name* **Configuration**.
   - On UNIX systems, execute `sh Install_Home/bin/configwizard` on the terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.
4. Complete the following steps on the **FTP/SCP/SFTP Server** screen.
   a. Choose one of the following options:
      - Select **Built-in FTP/SCP/SFTP Server** to configure an internal FTP/SCP/SFTP server and select one of the following options:
      - Select **Built-in FTP Server** to configure an internal FTP server
        The internal FTP server uses a default account and port 21. You can configure your own account from the **Options** dialog box. For instructions, refer to "Configuring an internal FTP server" on page 167.
      - Select **Built-in SCP/SFTP Server** to configure an internal SCP/SFTP server
        The internal SCP/SFTP server uses a default account and port 22. You can configure your own account from the **Options** dialog box. For instructions, refer to "Configuring an internal SCP or SFTP server" on page 167.
      - Select **External FTP/SCP/SFTP Server** to configure an external FTP server.
        You can configure the external FTP server settings from the **Options** dialog box. For instructions, refer to "Configuring an external FTP, SCP, or SFTP server" on page 168.

   b. Click **Next**.

   If port 21 or 22 is busy, a message displays. Click **OK** to close the message and continue. Once the Management application is configured, make sure port 21 or 22 is free and restart the server to start the FTP/SCP/SFTP service.

   NOTE
   If you use an FTP/SCP/SFTP server which is not configured on the same machine as the Management application, the Firmware Repository feature will not be available.
5. Complete the following steps on the **Server IP Configuration** screen.

   NOTE
   If the Management server or client has multiple Network Interface Cards and if any of these interfaces are not plugged in, you must disable them; otherwise, the following features do not work properly:
   Server impact
   - Configuration wizard (does not display all IP addresses)
   - Trap and Syslog auto registration
   - Report content (Ipconfiguration element does not display all server IP addresses)
   - Network OS configuration backup through FTP
   - Trace dump through FTP
   Client impact
   - Options dialog box (does not display all IP addresses)

- Firmware import and download dialog box
- Firmware import for Fabric OS and Network OS products
- FTP button in Technical Support Repository dialog box
- Technical supportSave of Fabric OS, Network OS, and Host products through FTP

a. Select an address from the **Server IP Configuration** list.

b. Select an address from the **Switch - Server IP Configuration Preferred Address** list.

> NOTE
> The host name does not display in the list if it contains invalid characters. Valid characters include alphanumeric and dash (-) characters. The IP address is selected by default.

If DNS is not configured for your network, do not select the “hostname” option from the **Server IP Configuration** list. Selecting the “hostname” option prevents clients and devices from communicating with the server.

c. Select an IP address from the **Switch - Server IP Configuration Preferred Address** list. The preferred IP address is used for switch and server communication.

or

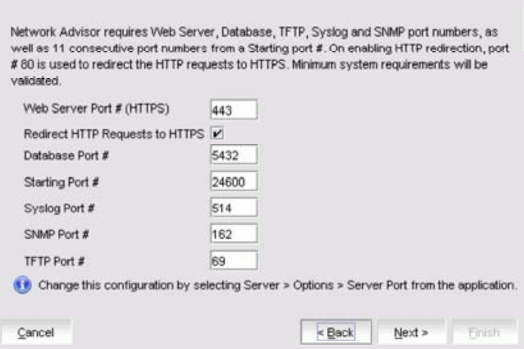
Select **Any** from the **Switch - Server IP Configuration Preferred Address** list to enable switch and server communication with one of the reachable IP address present in the server. By default, **Any** option is selected.

If you select a specific IP address from the **Server IP Configuration** screen and the selected IP address changes, you will not be able to connect to the server. To change the IP address, refer to “Configuring an explicit server IP address” on page 152.

d. Click **Next**.

6. Complete the following steps on the **Server Configuration** screen.

FIGURE 4 Server Configuration screen



Network Advisor requires Web Server, Database, TFTP, Syslog and SNMP port numbers, as well as 11 consecutive port numbers from a Starting port #. On enabling HTTP redirection, port # 80 is used to redirect the HTTP requests to HTTPS. Minimum system requirements will be validated.

Web Server Port # (HTTPS)	443
Redirect HTTP Requests to HTTPS	☑
Database Port #	5432
Starting Port #	24600
Syslog Port #	514
SNMP Port #	162
TFTP Port #	69

Change this configuration by selecting Server > Options > Server Port from the application.

a. Enter a port number in the **Web Server Port # (HTTPS)** field (default is 443).

b. Enable HTTP redirection to HTTPS by selecting the **Redirect HTTP Requests to HTTPS** check box.

When you enable HTTP redirection, the server uses port 80 to redirect HTTP requests to HTTPS. You can configure the server port settings from the **Options** dialog box (**Server Port** pane). For instructions, refer to “Configuring the server port” on page 171.

c. Enter a port number in the **Database Port #** field (default is 5432).

d. Enter a port number in the **Starting Port Number** field (default is 24600).

NOTE
For Professional software, the server requires 11 consecutive free ports beginning with the starting port number.

NOTE
For Trial and Licensed software, the server requires 11 consecutive free ports beginning with the starting port number.

e. Enter a port number in the **Syslog Port Number** field (default is 514).

NOTE
If the default syslog port number is already in use, you will not receive any syslog messages from the device. To find and stop the process currently running on the default Syslog port number, refer to the *Installation and Migration Guide*.

f. Enter a port number in the **SNMP Port Number** field (default is 162).

g. Click **Next**.

If you enter a syslog port number already in use, a message displays. Click **No** on the message to remain on the **Server Configuration** screen and edit the syslog port number (return to step 6a). Click **Yes** to close the message and continue with step 7.

If you enter a port number already in use, a Warning displays next to the associated port number field. Edit that port number and click **Next**.

7. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.
8. Complete the following steps on the **Start Server** screen:

h. Click **Finish**.

After all of the services (Server and Client) are started, the **Log In** dialog box displays.

9. Click **Yes** on the restart server confirmation message.
10. Choose one of the following options:

- If you configured authentication to CAC, enter your PIN in the **CAC PIN** field.
- If you configured authentication to the local database, an external server (RADIUS, LDAP, or TACACS+) or a switch, enter your user name and password.

  The defaults are **Administrator** and **password**, respectively.

NOTE
Do not enter *Domain\User_Name* in the **User ID** field for LDAP server authentication.

11. Click **Login**.
12. Click **OK** on the Login Banner.

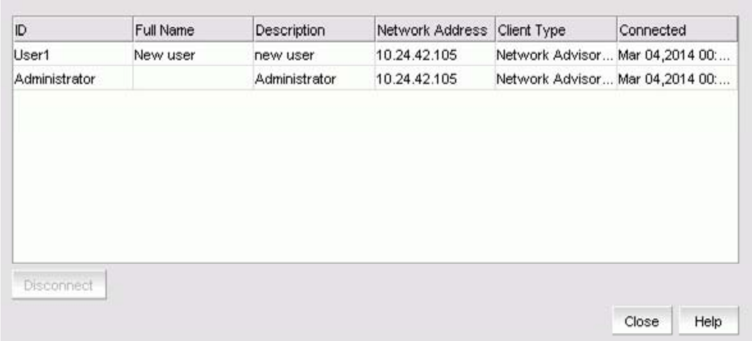
Viewing active sessions

To view the Management application active sessions, complete the following steps.

1. Select **Server > Active Sessions**.

   The **Active Sessions** dialog box displays (Figure 5).

FIGURE 5 Active Sessions dialog box



ID	Full Name	Description	Network Address	Client Type	Connected
User1	New user	new user	10.24.42.105	Network Advisor...	Mar 04,2014 00:...
Administrator		Administrator	10.24.42.105	Network Advisor...	Mar 04,2014 00:...

2. Review the active session information.

   The following information displays:

   - **ID** — Displays the name of the user (for example, Administrator).
   - **Full Name** — Displays the full name of the user.
   - **Description** — Displays the description of the user (for example, Operator).
   - **Network Address** — Displays the network address of the user.
   - **Client Type** — Displays the type of Management application client.
   - **Connected** — Displays the date and time the user connected to the server.

3. Click **Close**.

Disconnecting users

To disconnect a user, complete the following steps.

1. Select **Server > Active Sessions**.

   The **Active Sessions** dialog box displays.

2. Select the user you want to disconnect and click **Disconnect**.

3. Click **Yes** on the confirmation message.

   The user you disconnected receives the following message:

   The Client has been disconnected by *User_Name* from *IP_Address* at *Disconnected_Date_and_Time*.

4. Click **Close**.

   When you disconnect a client using the **Active Sessions** dialog box, the following event displays in the Master Log: Disconnect Client *User_Name @ IP_Address*.

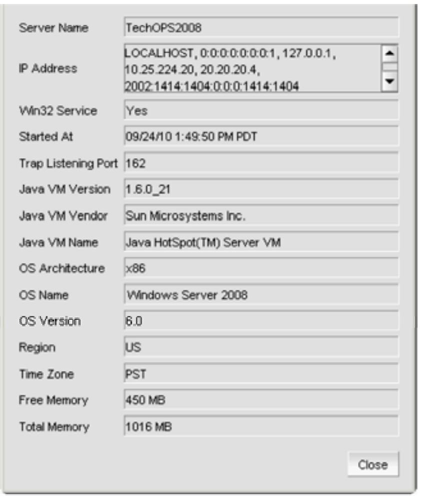
Viewing server properties

To view the Management application server properties, complete the following steps.

1. Select **Server > Server Properties**.

   The **Server Properties** dialog box displays.

FIGURE 6 Server Properties dialog box



Server Name	TechOPS2008
IP Address	LOCALHOST, 0:0:0:0:0:0:0:1, 127.0.0.1, 10.25.224.20, 20.20.20.4, 2002:1414:1404:0:0:0:1414:1404
Win32 Service	Yes
Started At	09/24/10 1:49:50 PM PDT
Trap Listening Port	162
Java VM Version	1.6.0_21
Java VM Vendor	Sun Microsystems Inc.
Java VM Name	Java HotSpot(TM) Server VM
OS Architecture	x86
OS Name	Windows Server 2008
OS Version	6.0
Region	US
Time Zone	PST
Free Memory	450 MB
Total Memory	1016 MB

2. Review the information.

TABLE 6 Server Properties

Field/Component	Description
Free Memory	The amount of free memory on the server.
IP Address	The IP address in IPv4 or IPv6 format.
Win32 Service	Specifies whether the Win32 service is available on the server. On UNIX servers, displays as “No”.
Java VM Name	The Java Virtual Machine name.
Java VM Vendor	The Java Virtual Machine vendor.
Java VM Version	The Java Virtual Machine version running on the server.
Server Name	The server’s name.
OS Architecture	The operating system architecture on the server.
OS Name	The name of the operating system running on the server.
OS Version	The operating system version running on the server.
Region	The server’s geographical region.
Started At	The time the server was started.
Time Zone	The server’s time zone.
Total Memory	The total amount of memory on the server.
Trap Listening Port	The number of the UDP port that listens for SNMP traps.

3. Click **Close** to close the **Server Properties** dialog box.

Viewing port status

The **Port Status** dialog box enables you to determine the availability of ports required for key Management application features. You can view the port status for the following ports:

- CIM Indication for Event Handling — Port 24618
- CIM Indication for HCM Proxy — Port 24619

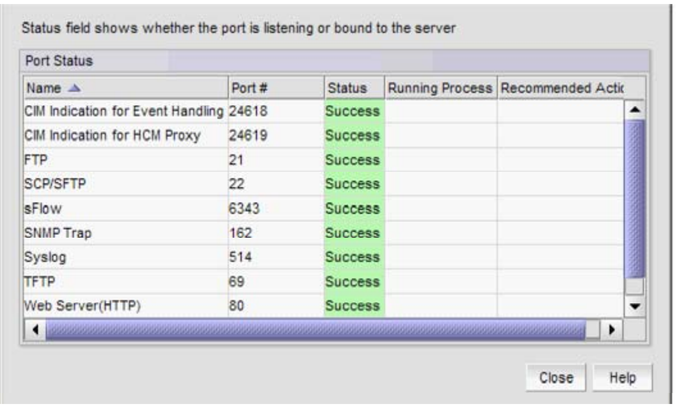
- FTP — Port 21
- SCP/SFTP — Port 22
- sFlow — Port 6343
- SNMP Trap — Port 162
- Syslog — Port 514
- TFTP — Port 69
- Web Server (HTTP) — Port 80
- Web Server (HTTPS) — Port 443

To view the port status, complete the following steps.

1. Click the port status icon (🖥).

   The **Port Status** dialog box displays.

   FIGURE 7 Port Status dialog box



Status field shows whether the port is listening or bound to the server

Port Status

Name ▲	Port #	Status	Running Process	Recommended Actic
CIM Indication for Event Handling	24618	Success		
CIM Indication for HCM Proxy	24619	Success		
FTP	21	Success		
SCP/SFTP	22	Success		
sFlow	6343	Success		
SNMP Trap	162	Success		
Syslog	514	Success		
TFTP	69	Success		
Web Server(HTTP)	80	Success		

2. Review the port status details:
   - **Name** — The Port name. Options include CIM Indication for Event Handling, CIM Indication for HCM Proxy, FTP, SCP/SFTP, sFlow, SNMP Trap, Syslog, TFTP, Web Server (HTTP), and Web Server (HTTPS).
   - **Port #** — The required port number.
   - **Status** — The status of the port. The status options are as follows:
     - Success — The port is listening or bound to the server.
     - Failed — The port fails to listen or bind to the server. It is occuppied by another process.
     - Paritally Failed — The port is used by the server as well as other applications.
     - Disabled (external FTP port only) — This is considered a normal status.
   - **Running Process** – The name of the process using the port (not the Management applciation). Blank when the port is only used by the Management applciation server. If multiple processes occupy the same port, the process names display in a comma-separated list.
   - **Recommended Actions** — Suggested action to take to resolve the issues.
3. Click **Close**.