



CHAPTER 5

Using the Network Navigator

To manage a network entity—Service Control Engine (SCE) platform, Subscriber Manager (SM), or Collection Manager (CM)—from the Console, you must first define it as a device in the Network Navigator.

This chapter describes how to use the Network Navigator tool to create a model of all local and remote sites and devices that are part of the Cisco Service Control solution, how to manage the devices remotely, and other functionality that is part of the Network Navigator tool.

The Usage Analysis wizard, which can be used to create a simple model of devices and connect to them, is also described in this chapter.

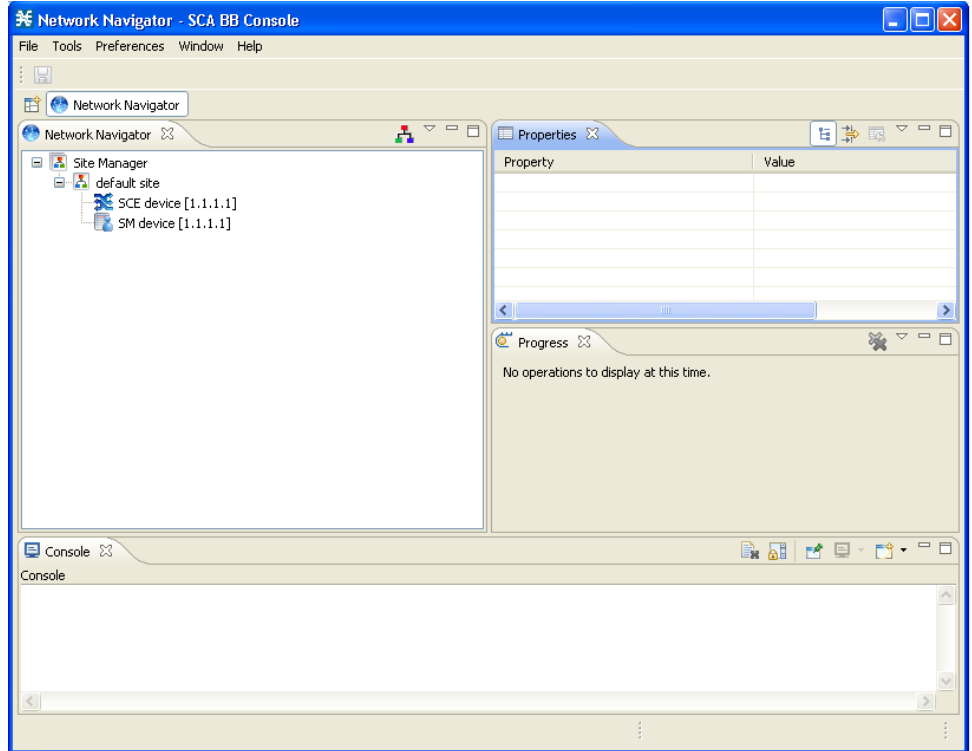
- [The Network Navigator Tool, page 5-1](#)
- [Managing Sites, page 5-2](#)
- [Managing Devices, page 5-6](#)
- [Working with Network Navigator Configuration Files, page 5-30](#)
- [Network Settings Requirements, page 5-34](#)

The Network Navigator Tool

The Network Navigator tool contains four views:

- Network Navigator view—Displays, in the Site Manager tree, all sites and devices that you have defined as part of your system
- Properties view—Displays the editable properties of the node selected in the Site Manager tree in the Network Navigator view
- ProgressView view—When you perform an operation on a site or device in the Site Manager tree, displays a progress bar
- Console view—Displays log messages concerning actions performed in the Network Navigator tool

Figure 5-1 Network Navigator



Managing Sites

You can manage an SCE, SM, or CM from the Console only if the network entity is defined as a device in the Network Navigator. After a device is added to the Network Navigator, you can perform management and monitoring operations on the device.

You can also perform operations on a group of devices. For example, you can apply the same service configuration to a group of SCE platforms. The Network Navigator allows you to group devices by adding them under the same site. A site is a group of devices that can be managed together. At installation, the Network Navigator contains a default site with no devices. You can add devices to this site or add additional sites, as described in the following sections.

Grouping devices in sites can also help to manage the passwords for these devices (see [Password Management](#), page 5-6).

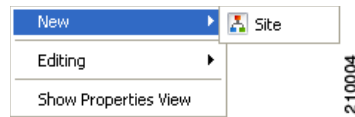
- [How to Add a Site to the Site Manager](#), page 5-2
- [How to Add Devices to a Site](#), page 5-3
- [How to Delete Sites](#), page 5-6

How to Add a Site to the Site Manager

Before adding devices, you must add your sites to the Site Manager.

-
- Step 1** In the Network Navigator view, right-click the Site Manager node.

A popup menu appears.



Step 2 From the menu, select **New > Site**.

A new Site node is added to the Site Manager.

Step 3 In the Properties view, enter a name for the site in the Name cell.

Step 4 (Option) In the Version cell, enter a version number.

How to Add Devices to a Site

You can add SCE, SM, CM, or database devices to a site.

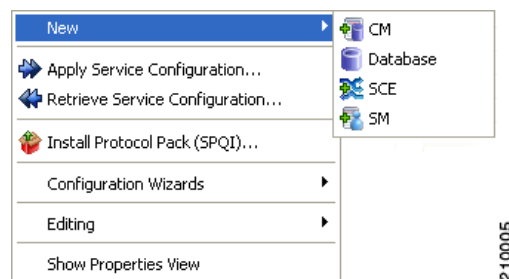
- [How to Add SCE Devices to a Site, page 5-3](#)
- [How to Add SM Devices to a Site, page 5-4](#)
- [How to Add CM Devices to a Site, page 5-4](#)
- [How to Add Database Devices to a Site, page 5-4](#)
- [How to Delete Devices, page 5-5](#)

How to Add SCE Devices to a Site

To use the Network Navigator to configure, monitor, and update the software of an SCE platform, you must first add the SCE platform to a site.

Step 1 In the Site Manager tree, right-click a site.

A popup menu appears.



Step 2 From the menu, select **New > SCE**.

The Create New SCE wizard appears.

Step 3 In the Address field, enter the IP address of the SCE.

Step 4 (Option) In the Name field, enter a meaningful name for the SCE.

Step 5 Click **Finish**.

The Create New SCE wizard closes.

The new device is added to the site.

How to Add SM Devices to a Site

To use the Network Navigator to configure, monitor, and update the software of an SM, you must first add the SM to a site.

- Step 1** In the Site Manager tree, right-click a site.
A popup menu appears.
 - Step 2** From the menu, select **New > SM**.
The Create New SM wizard appears.
 - Step 3** In the Address field, enter the IP address of the SCMS-SM.
 - Step 4** (Option) In the Name field, enter a meaningful name for the SM.
 - Step 5** Click **Finish**.
The Create New SM wizard closes.
The new device is added to the site.
-

How to Add CM Devices to a Site

To use the Network Navigator to monitor a CM, you must first add the CM to a site.

- Step 1** In the Site Manager tree, right-click a site.
A popup menu appears.
 - Step 2** From the menu, select **New > CM**.
The Create New CM wizard appears.
 - Step 3** In the Address field, enter the IP address of the CM.
 - Step 4** (Option) In the Name field, enter a meaningful name for the CM.
 - Step 5** Click **Finish**.
The Create New CM wizard closes.
The new device is added to the site.
-

How to Add Database Devices to a Site

To use the Reporter tool to produce reports, you must first connect to a database.

- Step 1** In the Site Manager tree, right-click a site.

A popup menu appears.

Step 2 From the menu, select **New > Database**.

The Create New Database wizard appears.

Step 3 In the Address field, enter the IP address of the database.

Step 4 (Option) In the Name field, enter a meaningful name for the database.

Step 5 From the Database type drop-down list, select a database type.

Step 6 (Option) Check the **Enable Advanced Settings** check box and enter new values in the Url, Driver, User, and Password fields.

Step 7 Click **Finish**.

The Create New Database wizard closes.

The new device is added to the site.

How to Delete Devices

Step 1 In the Site Manager tree, right-click a device.

A popup menu appears.

Step 2 From the menu, select **Delete**.

The device is deleted and removed from the Site Manager tree.

How to Delete Sites

-
- Step 1** In the Site Manager tree, right-click a site in the Site Manager tree.
- A popup menu appears.
- Enter your password if prompted.
- Step 2** From the menu, select **Delete**.
- The site and all its devices are deleted and the site is removed from the Site Manager tree.
-

Managing Devices

The Network Navigator allows you to manage SCE, SM, CM, and database devices.

**Note**

The Usage Analysis wizard allows you to create a simple model of devices and connect to them. (See [How to Use the Usage Analysis Wizard, page 4-18.](#))

- [Password Management, page 5-6](#)
- [Managing SCE Devices, page 5-7](#)
- [Managing SM Devices, page 5-23](#)
- [Managing CM Devices, page 5-27](#)
- [Managing Database Devices, page 5-27](#)

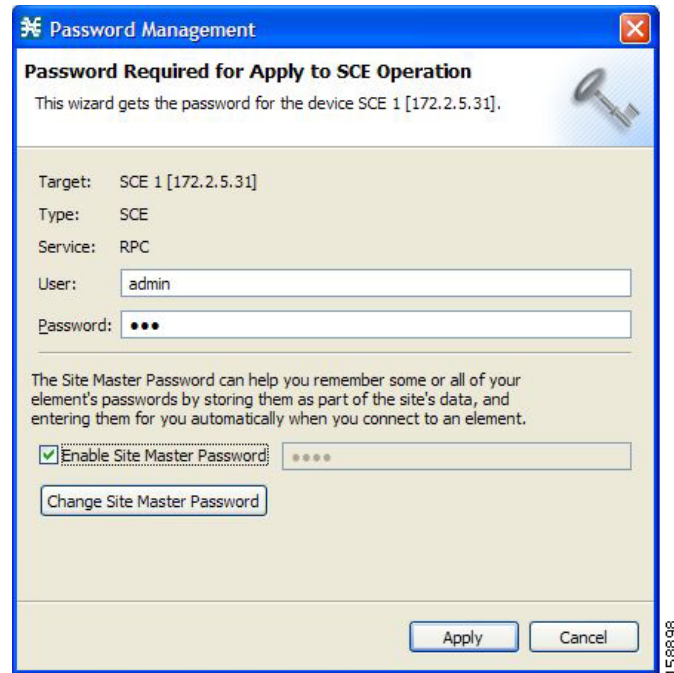
Password Management

Normally, before you can access a device (SCE, SM, CM, or database), you must enter its password. When you try to perform any operation on a site device, the Network Navigator first asks for the device username and password. (Repeating the same operation on the same device does not always require a second entry of the password.)

When performing operations on multiple devices, password entry can become tedious. The Site Master Password can help you remember some or all of your element's usernames and passwords by storing them as part of the site's data, and entering them for you automatically when you connect to an element.

The Site Master Password protects saved usernames and passwords in the password manager. The Console prompts you for the site's master password when you wish to activate the site password manager. If you have multiple sites, each site will require a separate master password.

Figure 5-2 Password Management



For each site, when the Password Management dialog box appears, check the **Enable Site Master Password** check box.

Managing SCE Devices

- [How to Configure SCE and CM Devices Using a Wizard, page 5-7](#)
- [How to Generate Tech Support Info Files for SCE Devices, page 5-15](#)
- [How to Retrieve the Online Status of SCE Devices, page 5-16](#)
- [How to Install a Protocol Pack, page 5-17](#)
- [How to Apply Service Configurations to SCE Devices, page 5-19](#)
- [How to Retrieve Service Configurations from SCE Devices, page 5-21](#)
- [How to Install PQI Files on SCE Devices, page 5-21](#)
- [How to Install an SCE OS Software Package on SCE Devices, page 5-22](#)


How to Configure SCE and CM Devices Using a Wizard

The Network Navigator Device wizard allows you to configure SCA and CM devices and connect to them.

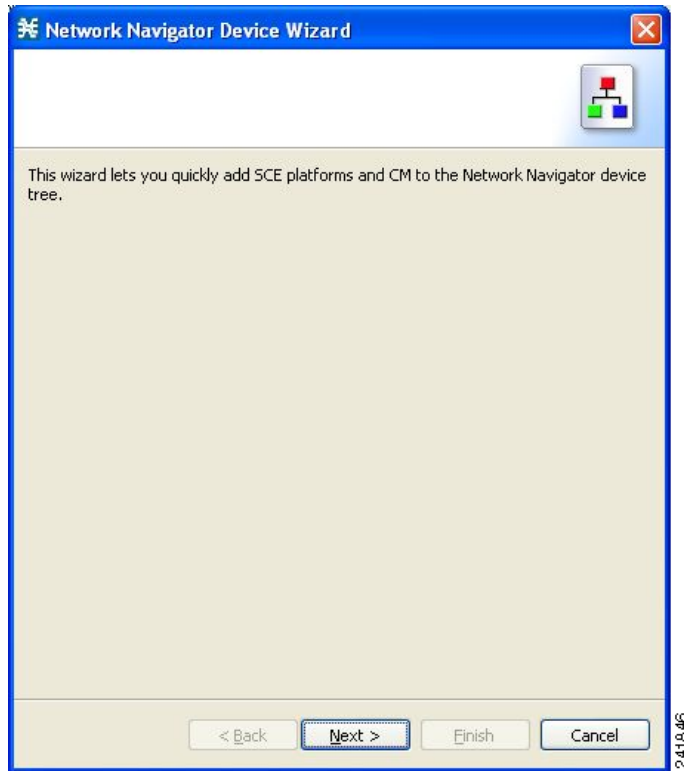


Note

If they do not already exist, devices defined in the wizard are added to the default site in the Site Manager tree.

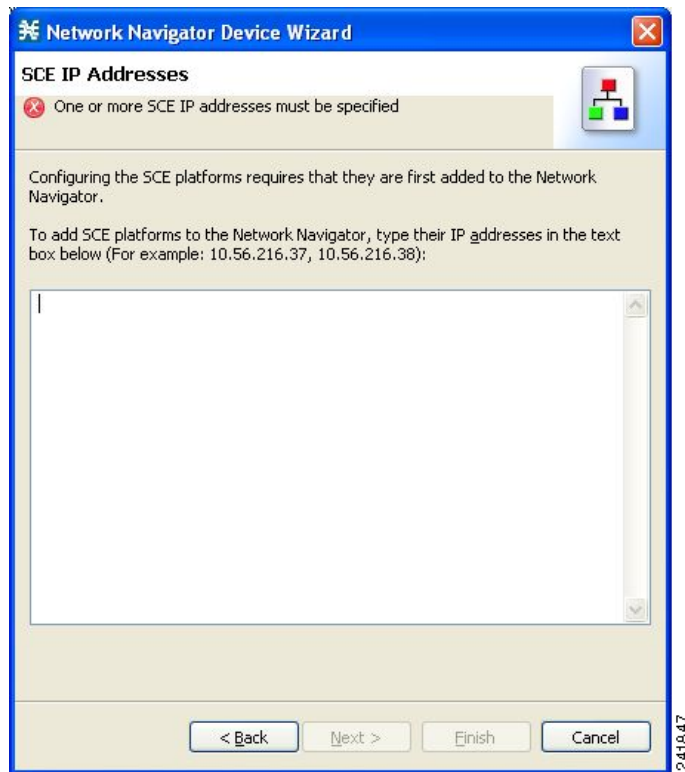
Step 1 In the Network Navigator view toolbar, click  (**Configure SCE and CM devices**).

The Welcome page of the Network Navigator Device wizard appears.



Step 2 Click **Next**.

The SCE IP Addresses page of the Network Navigator Device wizard opens.

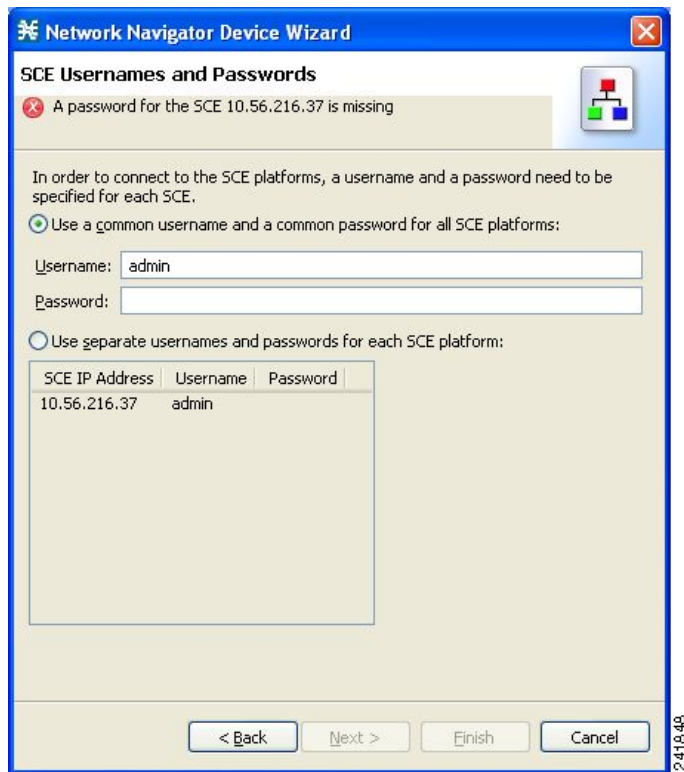


- Step 3** In the edit box, enter the IP addresses of the SCE devices that should be added to the model. If you started from the Network Navigator, the IP addresses of the SCE devices that you selected are displayed in the edit box. You can add additional addresses.



Note You can work with up to 20 SCE devices at one time using the wizard.

- Step 4** Click **Next**.
The SCE Usernames and Passwords page of the Network Navigator Device wizard opens.



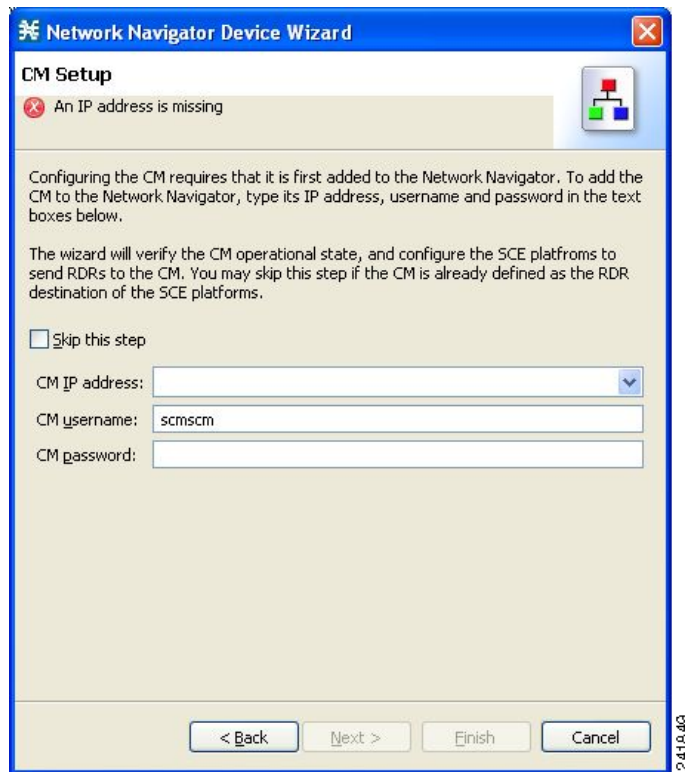
Step 5 Enter the user names and passwords for the SCE devices.

Do one of the following:

- To use the same user name and password for all the SCE devices that you are adding, enter the user name in the Username field and the password in the Password field.
- To provide a different user name and password pair for each SCE device, check the **Use separate usernames and passwords for each SCE device** radio button, and, for each SCE device, enter the user name and password in the appropriate cell of the SCE device table.

Step 6 Click **Next**.

The Setting CM devices page of the Network Navigator Device wizard opens.



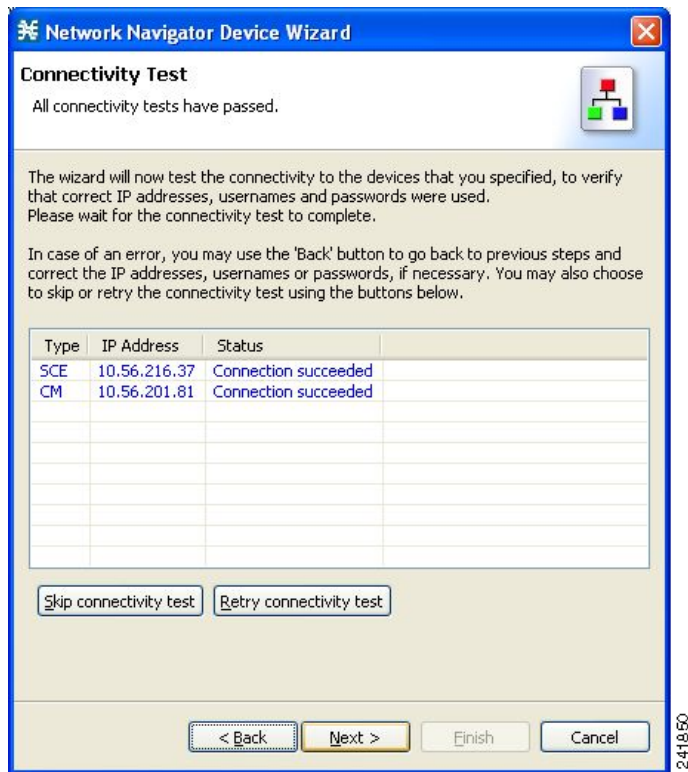
Step 7 Define the SCSM Collection Manager (CM) to use with this configuration.

Do one of the following:

- Enter the IP address, user name, and password of the CM device in the appropriate fields.
If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.
- Check the **Skip this step** check box.

Step 8 Click **Next**.

The Connectivity Test page of the Network Navigator Device wizard opens.



The wizard tests to see that the connections to the defined devices can be made.

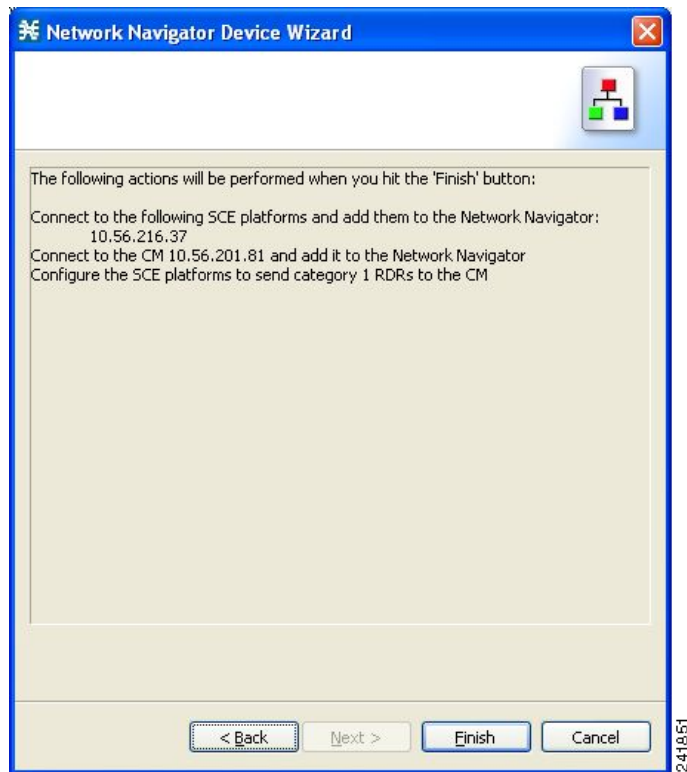


Note

If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device) an error is displayed next to the device. You can skip these tests by clicking **Skip Connections**. The connections will be validated when you click **Finish** at the end of the wizard.

Step 9 Click **Next**.

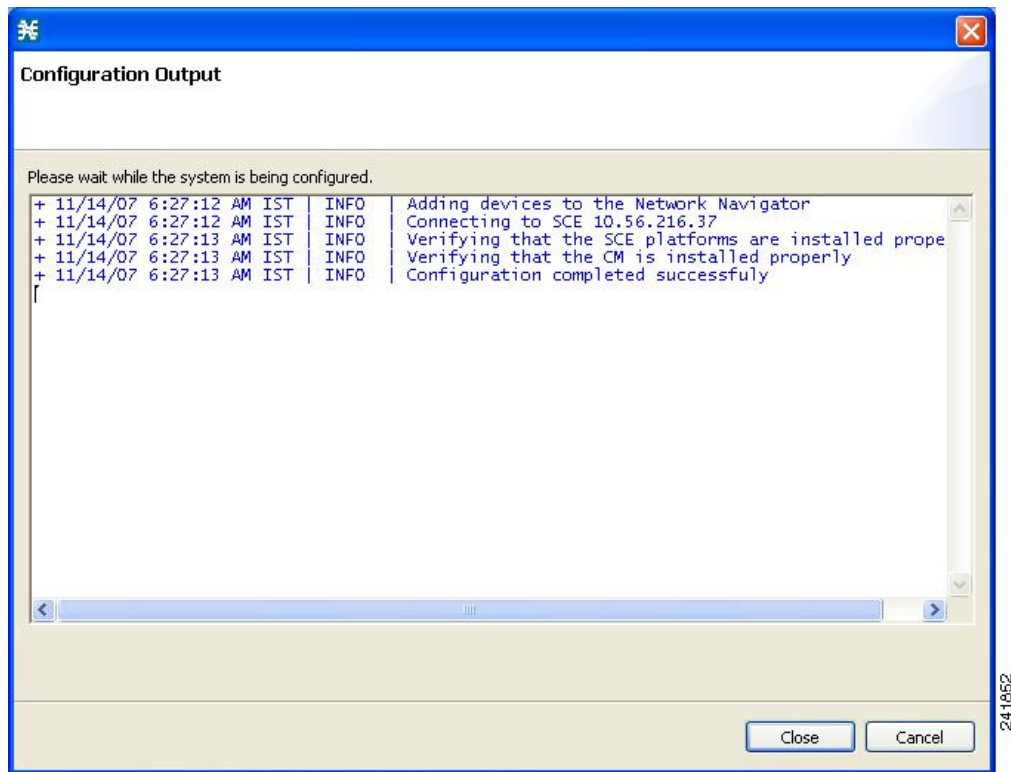
The Confirmation page of the Network Navigator Device wizard opens.



The actions that the wizard is about to take are listed in the page.

Step 10 Click **Finish**.

The Configuration Output page of the Network Navigator Device wizard opens.



New devices are added to the default site in the Site Manager tree in the Network Navigator.



The wizard attempts to connect to all devices that you defined. The operation fails if:

- The wizard cannot connect to any of the SCE devices that you listed in Step 3.
- You defined a CM in Step 7, but the wizard cannot connect to it.

If you defined a CM in Step 7, the SCE devices are configured so that the only category 1 RDR destination is the CM.



Note

RDR categories are the mechanism by which different types of RDRs can be sent to different collectors. For more information about RDR categories, see the “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

A new service configuration is created:

- Report Only mode.

- The maximum Transaction RDR rate is set as the default value (250) divided by the number of SCE devices. (To configure the Transaction RDR see [How to Manage Transaction RDRs, page 8-4](#); the content and structure of the Transaction RDR is listed in "Transaction RDR" in the "Raw Data Records: Formats and Field Contents" chapter of the *Cisco Service Control Application for Broadband Reference Guide*.)

Step 11 Click **Finish**.

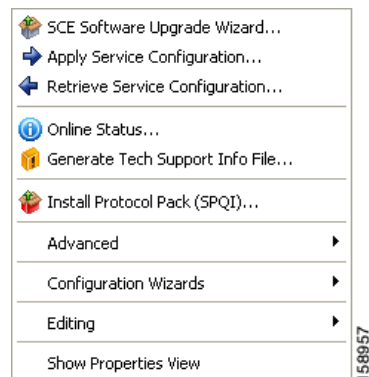
The Network Navigator Device wizard closes.

How to Generate Tech Support Info Files for SCE Devices

This operation generates the SCE platform's support file, for the use of Cisco technical support staff.

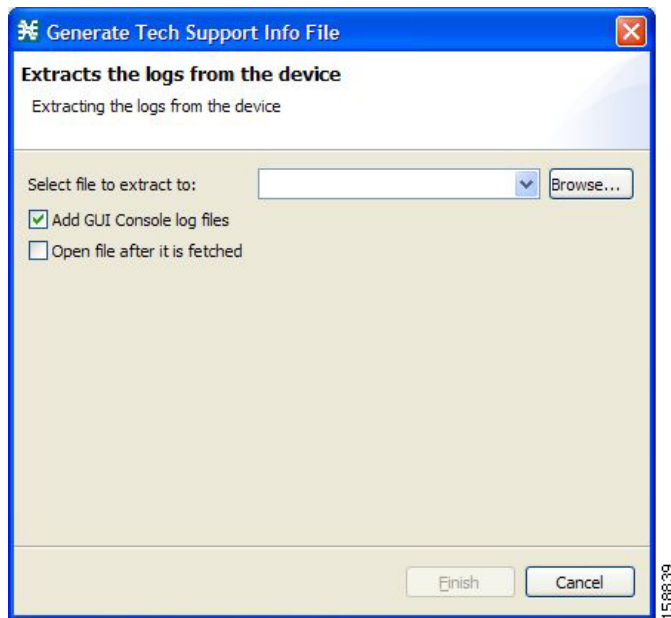
Step 1 In the Site Manager tree, right-click an SCE device.

A popup menu appears.



Step 2 From the menu, select **Generate Tech Support Info File**.

The Generate Tech Support Info File dialog box appears.

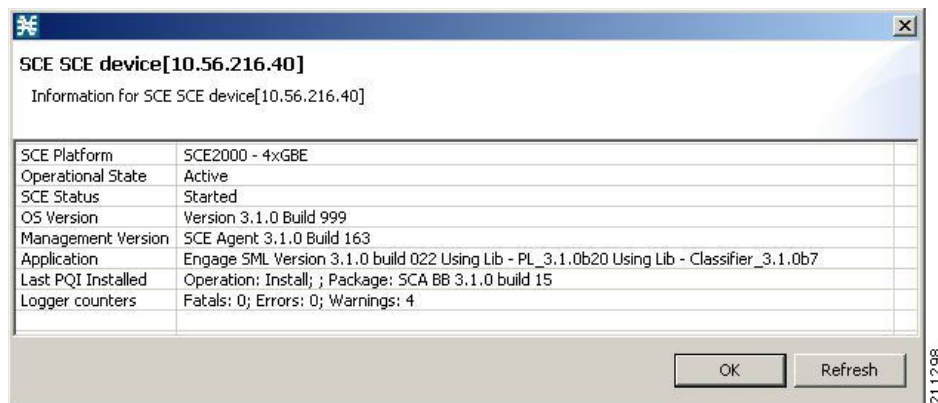


- Step 3** Click **Browse**.
- A Select File dialog box appears.
- Step 4** Browse to the folder where you want to save the tech support info file.
- Step 5** In the File name field, enter a new file name, or select an existing ZIP file.
- Step 6** Click **Open** to select the file.
- If the file exists, it will be overwritten when you generate the tech support info.
- The Select File dialog box closes.
- Step 7** (Option) To add log files to the output tech support info file, check the **Add GUI Console log files** check box.
- Step 8** (Option) Check the **Open file after it is fetched** check box.
- Step 9** Click **Finish**.
- The Generate Tech Support Info File dialog box closes.
- A Password Management dialog box appears.
- Step 10** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)
- Step 11** Click **Generate**.
- The Password Management dialog box closes.
- A Generate tech support info file progress bar appears.
- The file is generated.

How to Retrieve the Online Status of SCE Devices

This operation provides information about the SCE platform's current software version and operational status.

- Step 1** In the Site Manager tree, right-click an SCE device.
A popup menu appears.
- Step 2** From the menu, select **Online Status**.
A Password Management dialog box appears.
- Step 3** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)
- Step 4** Click **Extract**.
The Password Management dialog box closes.
An Extracting info progress bar appears.
The SCE online status is retrieved.



211298

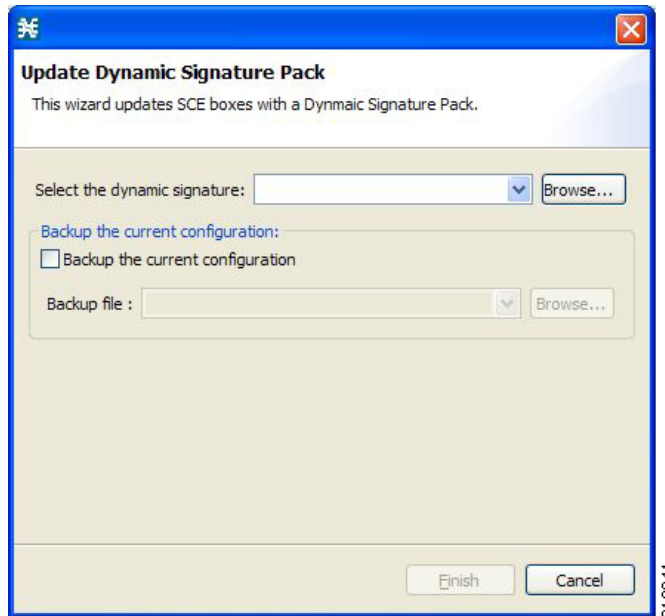
How to Install a Protocol Pack

You can install a protocol pack on a single SCE platform, on selected SCE platforms, or on all SCE platforms at one or more selected sites. For more information about protocol packs, see [Working with Protocol Packs, page 4-9](#).

- [How to Install a Protocol Pack on a Single SCE Platform, page 5-17](#)
- [How to Install a Protocol Pack on Multiple SCE Platforms, page 5-18](#)

How to Install a Protocol Pack on a Single SCE Platform


- Step 1** In the Site Manager tree, right-click the SCE where the protocol pack is to be installed.
- Step 2** From the popup menu that appears, select **Update Dynamic Signature Pack**.
The Update Dynamic Signature Pack dialog box appears.



- Step 3** Click **Browse**.
- A Select file dialog box appears.
- Step 4** From the Files of type drop-down list, select ***.spqi** or ***.dss**, according to the file to be installed.
- Step 5** Browse to the file to be installed.
- Step 6** Click **Open**.
- The Select file dialog box closes.
- Step 7** (Recommended) Check the **Backup the current configuration** check box, click **Browse**, and select a backup file.
- Step 8** Click **Finish**.
- A Password Management dialog box appears.
- Step 9** Enter the appropriate password.
- For more information, refer to [Password Management, page 5-6](#).
- Step 10** Click **Update**.
- The Password Management dialog box closes.
- An Update Dynamic Signature Pack progress bar appears.
- The service configuration on the SCE platform is updated.

How to Install a Protocol Pack on Multiple SCE Platforms

- Step 1** In the Site Manager tree, select sites or SCE devices where the protocol pack will be installed, and right-click one of them
- Step 2** From the popup menu that appears, choose **Update Dynamic Signature Pack**.
- The Update Dynamic Signature Pack dialog box appears.

- Step 3** Select the protocol pack to be installed.
- Step 4** (Recommended) Check the **Backup the current configuration** check box and select a backup directory.
-  **Note** The backup files will be named *backupPolicy_<SCE platform IP address>.pqb*.
- Step 5** Click **Finish**.
A separate Password Management dialog box appears for each SCE device that you selected.
- Step 6** For each SCE device, enter the password and click **Update**.
The protocol pack is installed on each SCE platform in turn.

How to Apply Service Configurations to SCE Devices

You can apply a service configuration to a single SCE platform, to selected SCE platforms, or to all SCE platforms at one or more selected sites.



Note The service configuration that you are applying must be open in the Service Configuration Editor.



Caution


If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Service Control Engine (SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform.

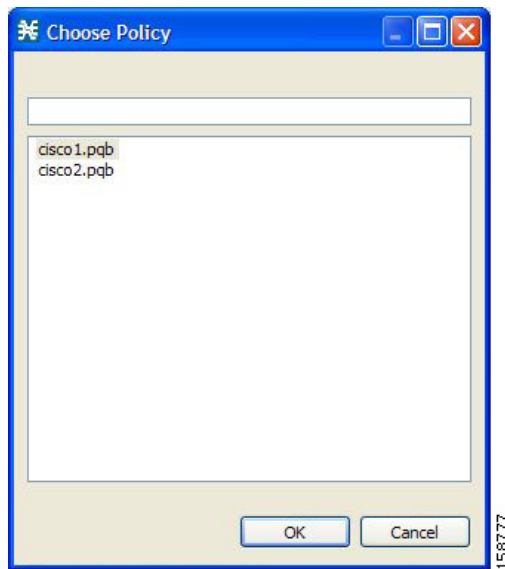
Workaround:

Disable anomaly-based detection of malicious traffic.
In the Network Traffic tab, select **Service Security**.
In the Service Security Dashboard, clear the **Enable anomaly detection** check box.

- [How to Apply a Service Configuration to a Single SCE Platform, page 5-19](#)
- [How to Apply a Service Configuration to Multiple SCE Platforms, page 5-20](#)

How to Apply a Service Configuration to a Single SCE Platform

- Step 1** In the Site Manager tree, right-click an SCE device.
A popup menu appears.
- Step 2** From the menu, select **Apply Service Configuration**.
The Choose Policy dialog box appears, listing all service configurations that are open in the Service Configuration Editor.
-  **Note** If only one service configuration is open in the Service Configuration Editor, a Password Management dialog box appears. Continue at Step 5. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)



Step 3 Select a service configuration from the list.

Step 4 Click **OK**.

A Password Management dialog box appears.

Step 5 Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)

Step 6 Click **Apply**.

The Password Management dialog box closes.

An Applying service configuration to SCE progress bar appears.

The service configuration is applied to the selected SCE platform.

How to Apply a Service Configuration to Multiple SCE Platforms

Step 1 In the Site Manager tree, select sites or SCE devices to which you are applying the service configuration and right-click one of them.

Step 2 From the popup menu that appears, select **Apply Service Configuration**.

The Choose Policy dialog box appears, listing all service configurations that are open in the Service Configuration Editor.



Note

If only one service configuration is open in the Service Configuration Editor, a Password Management dialog box appears. Continue at Step 4. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)

Step 3 Select a service configuration from the list and click **OK**.

A separate Password Management dialog box appears for each SCE device that you have selected.

Step 4 For each SCE device, enter the password and click **Apply**.

The service configuration is applied to each selected SCE platform in turn.

How to Retrieve Service Configurations from SCE Devices

You can retrieve service configurations from a single SCE platform, from selected SCE platforms, or from all SCE platforms at one or more selected sites.

- [How to Retrieve Service Configurations from a Single SCE Platform, page 5-21](#)
- [How to Retrieve Service Configurations from Multiple SCE Platforms, page 5-21](#)

How to Retrieve Service Configurations from a Single SCE Platform

- Step 1** In the Site Manager tree, right-click an SCE device.
- A popup menu appears.
- Enter your password if prompted.
- Step 2** From the menu, select **Retrieve Service Configuration**.
- A Password Management dialog box appears.
- Step 3** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)
- Step 4** Click **Retrieve**.
- The Password Management dialog box closes.
- A Retrieving from SCE progress bar appears.
- The service configuration is retrieved from the SCE platform and opened in the Service Configuration Editor.
-

How to Retrieve Service Configurations from Multiple SCE Platforms

- Step 1** In the Site Manager tree, select sites or SCE devices whose service configurations you want to retrieve, and right-click one of them.
- Step 2** From the popup menu that appears, select **Retrieve Service Configuration**.
- A separate Password Management dialog box appears for each SCE device that you have selected.
- Step 3** For each SCE device, enter the password and click **Retrieve**.
- The service configuration is retrieved from each SCE platform in turn, and is opened in the Service Configuration Editor.
-

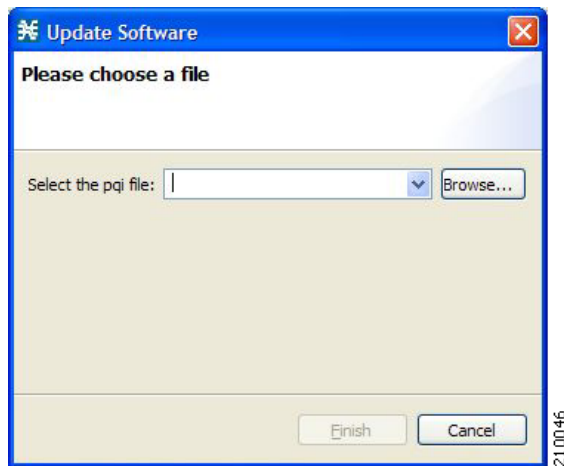
How to Install PQI Files on SCE Devices

This operation installs the Cisco Service Control Application for Broadband (SCA BB) on the SCE platform.

**Note**

Installing a PQI file usually takes a few minutes.

- Step 1** In the Site Manager tree, select an SCE device.
- Step 2** From the Console main menu, choose **Network > Install Application Software (PQI)**.
The Update Software dialog box appears.



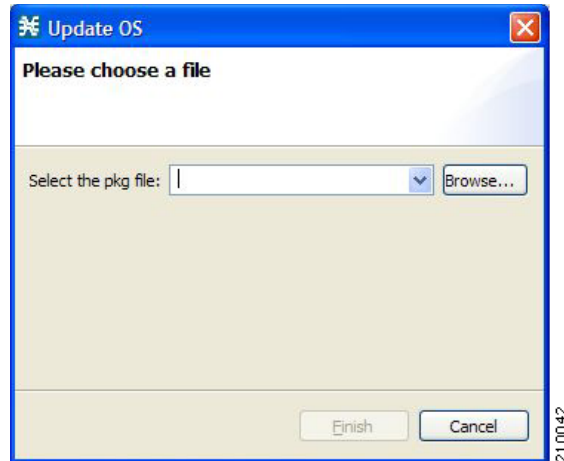
- Step 3** Click **Browse**.
A Select file dialog box appears.
- Step 4** Browse to the PQI file that you are installing.
- Step 5** Click **Open**.
The Select file dialog box closes.
- Step 6** Click **Finish**.
A Password Management dialog box appears.
- Step 7** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6.](#))
- Step 8** Click **Apply**.
The Password Management dialog box closes.
An Updating software to SCE progress bar appears.
The PQI file is installed on the selected SCE.

How to Install an SCE OS Software Package on SCE Devices

This operation installs the SCE OS software package (the operating system software and firmware of the SCE platform).

For more information, see “Upgrading SCE Platform Firmware” in the “Operations” chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

- Step 1** In the Site Manager tree, select an SCE device.
- Step 2** From the Console main menu, choose **Network > Upgrade SCE Platform Firmware (PKG)**.
The Update OS dialog box appears.



- Step 3** Click **Browse**.
A Select file dialog box appears.
- Step 4** Browse to the PKG file containing the OS that you are installing.
- Step 5** Click **Open**.
The Select file dialog box closes.
- Step 6** Click **Finish**.
A Password Management dialog box appears.
- Step 7** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)
- Step 8** Click **Apply**.
The Password Management dialog box closes.
An Updating software to SCE progress bar appears.
The PQI file is installed on the selected SCE.

Managing SM Devices

- [How to Generate Tech Support Info Files for SM Devices, page 5-23](#)
- [How to Retrieve the Online Status of SM Devices, page 5-24](#)
- [How to Connect to SM Devices, page 5-25](#)
- [How to Install PQI Files on SM Devices, page 5-26](#)

How to Generate Tech Support Info Files for SM Devices

This operation generates the SM's support file, for the use of Cisco technical support staff.

- Step 1** In the Site Manager tree, right-click an SM device.
A popup menu appears.



- Step 2** From the menu, select **Generate Tech Support Info File**.
The Generate Tech Support Info File dialog box appears.
- Step 3** Click **Browse**.
A Select File dialog box appears.
- Step 4** Browse to the folder where you want to save the tech support info file.
- Step 5** In the File name field, enter a new file name, or select an existing ZIP file.
- Step 6** Click **Open** to select the file.
If the file exists, it will be overwritten.
The Select File dialog box closes.
- Step 7** (Option) To add log files to the output tech support info file, check the **Add GUI Console log files check box**.
- Step 8** Check the **Open file after it is fetched** check box.
- Step 9** Click **Finish**.
The Generate Tech Support Info File dialog box closes.
A Password Management dialog box appears.
- Step 10** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)
- Step 11** Click **Generate**.
The Password Management dialog box closes.
A Generate tech support info file progress bar appears.
The file is generated.

How to Retrieve the Online Status of SM Devices

This operation provides information about the SM's current software version and operational status.

- Step 1** In the Site Manager tree, right-click an SM device.
A popup menu appears.
- Step 2** From the menu, select **Online Status**.

A Password Management dialog box appears.

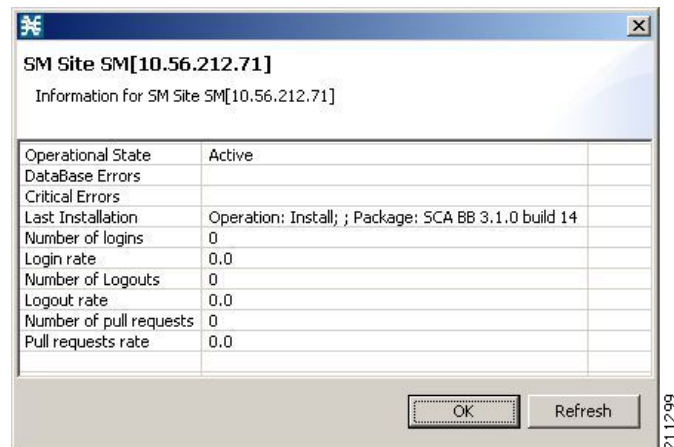
Step 3 Enter the appropriate password. (For more information, refer to [Password Management, page 5-6.](#))

Step 4 Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS-SM online status is retrieved.



How to Connect to SM Devices

In order to manage subscribers using the SM GUI tool, you must connect to an SM device.



Note

The SM GUI tool performs authentication on the SCMS-SM by opening a PRPC connection to port 14374 and attempting to log in using the username and password that you entered in the Password Management dialog box. If a PRPC server with this user is not running on the SCMS-SM, authentication will fail.

Step 1 In the Site Manager tree, right-click an SM device.

A popup menu appears.

Step 2 From the menu, select **Manage Subscribers**.

A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, refer to [Password Management, page 5-6.](#))

Step 4 Click **Connecting**.

The Password Management dialog box closes.

A Connecting to progress bar appears.

You connect to the SM, and the Console switches to the SM GUI tool.

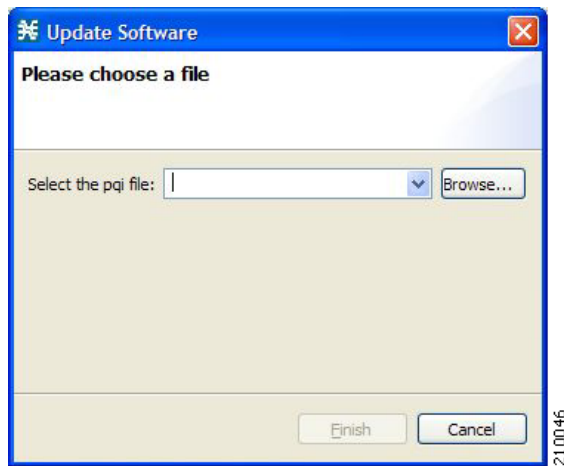
For an explanation of how to proceed, see [Using the Subscriber Manager GUI Tool, page 11-1](#).

How to Install PQI Files on SM Devices



Note Installing a PQI file usually takes a few minutes.

- Step 1** In the Site Manager tree, select an SM device.
- Step 2** From the Console main menu, choose **Network > Install Application Software (PQI)**.
The Update Software dialog box appears.



- Step 3** Click **Browse**.
A Select file dialog box appears.
- Step 4** Browse to the PQI file that you are installing.
- Step 5** Click **Open**.
The Select file dialog box closes.
- Step 6** Click **Finish**.
A Password Management dialog box appears.
- Step 7** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6](#).)
- Step 8** Click **Apply**.
The Password Management dialog box closes.
An Updating software to SM progress bar appears.
The PQI file is installed on the selected SM.

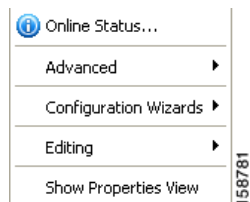
Managing CM Devices

You can configure CM devices using a wizard. (See [How to Configure SCE and CM Devices Using a Wizard, page 5-7.](#))

How to Retrieve the Online Status of CM Devices

This operation provides information about the CM's current software version and operational status.

- Step 1** In the Site Manager tree, right-click a CM device.
A popup menu appears.



- Step 2** From the menu, select **Online Status**.
A Password Management dialog box appears.
- Step 3** Enter the appropriate password. (For more information, refer to [Password Management, page 5-6.](#))
- Step 4** Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS-CM online status is retrieved.

For an example of a retrieved online status window (for an SCE platform), see [How to Retrieve the Online Status of SCE Devices, page 5-16.](#)

Managing Database Devices

How to Make Databases Accessible to the SCA Reporter

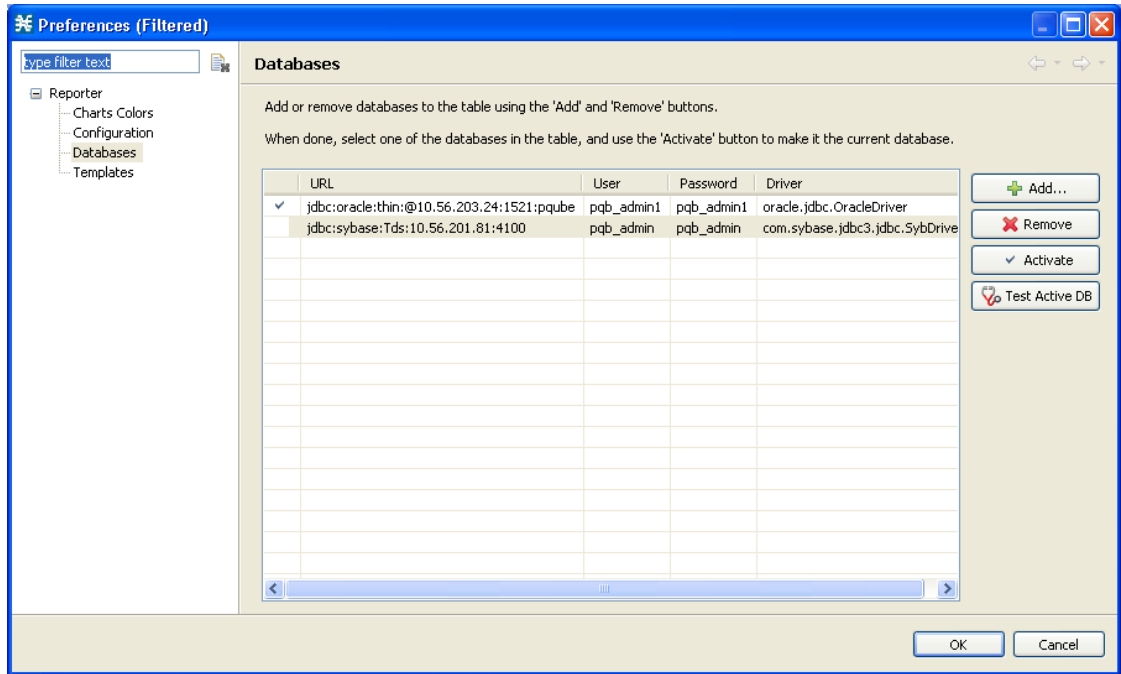
- The Reporter DB Configuration wizard allows you to connect the Reporter to a single database. (See [How to Use the Reporter DB Configuration Wizard, page 4-44.](#))
- An alternative procedure is described in “Configuring a Database Connection” in the “Using the SCA Reporter” chapter of the *Cisco Service Control Application Reporter User Guide*.

- Step 1** In the Site Manager tree, right-click a database device.
A popup menu appears.



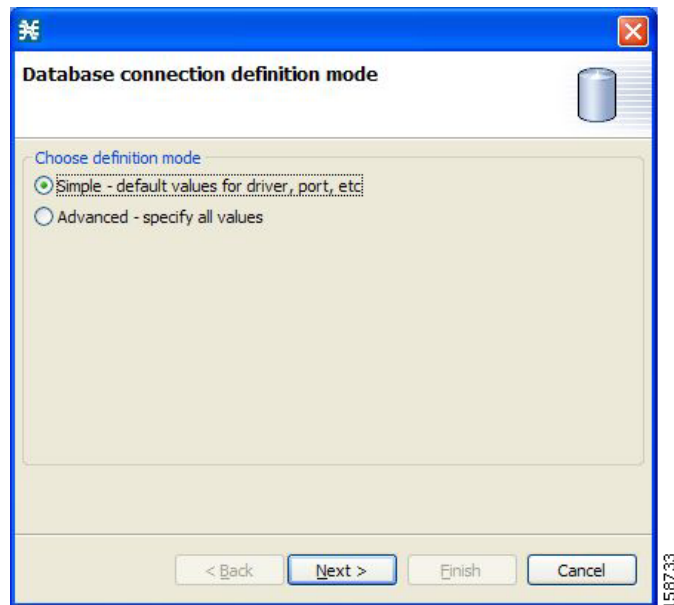
Step 2 From the menu, select **Add to Reporter**.

The Preferences dialog box appears.



Step 3 Click **Add**.

The Add Database wizard appears.



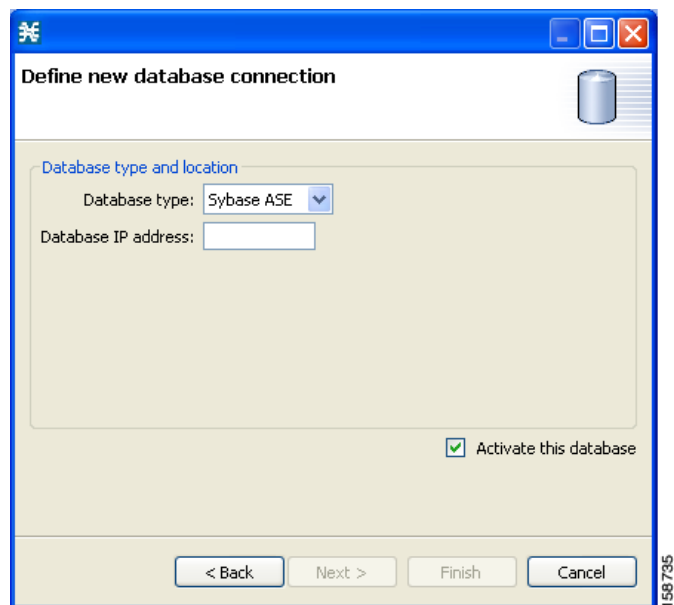
Step 4 Select one of the **Choose definition mode** radio buttons.

- **Simple**
- **Advanced**

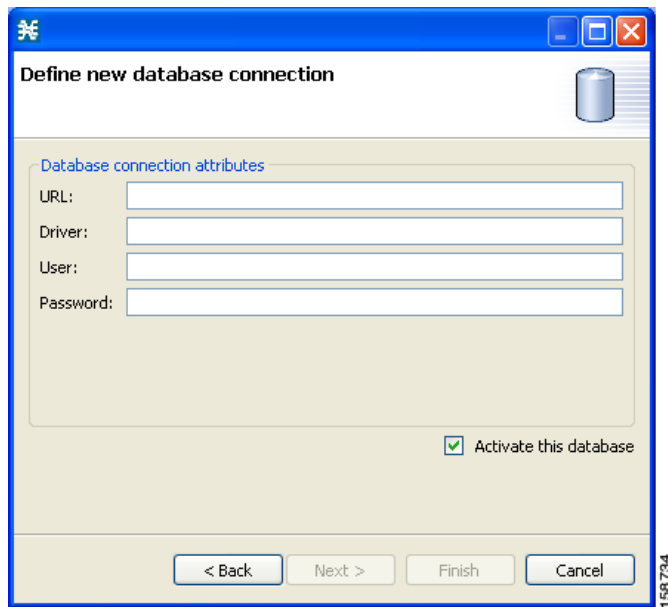
Step 5 Click **Next**.

The Define new database connection page of the Add Database wizard opens:

- If you selected Simple in Step 4, the Define new database connection page looks like this:



- If you selected Advanced in Step 4, the Define new database connection page looks like this:



Step 6 Fill in all the fields.

Step 7 Click **Finish**.

The Add Database wizard closes.

The definition of the database is added to the list in the Preferences dialog box.

Step 8 Repeat Steps 3 to 7 for other databases.

Step 9 If required, delete databases from the list in the Preferences dialog box.

Step 10 Make sure that the correct database is activated.

Step 11 Click **OK**.

The Preferences dialog box closes.

Working with Network Navigator Configuration Files

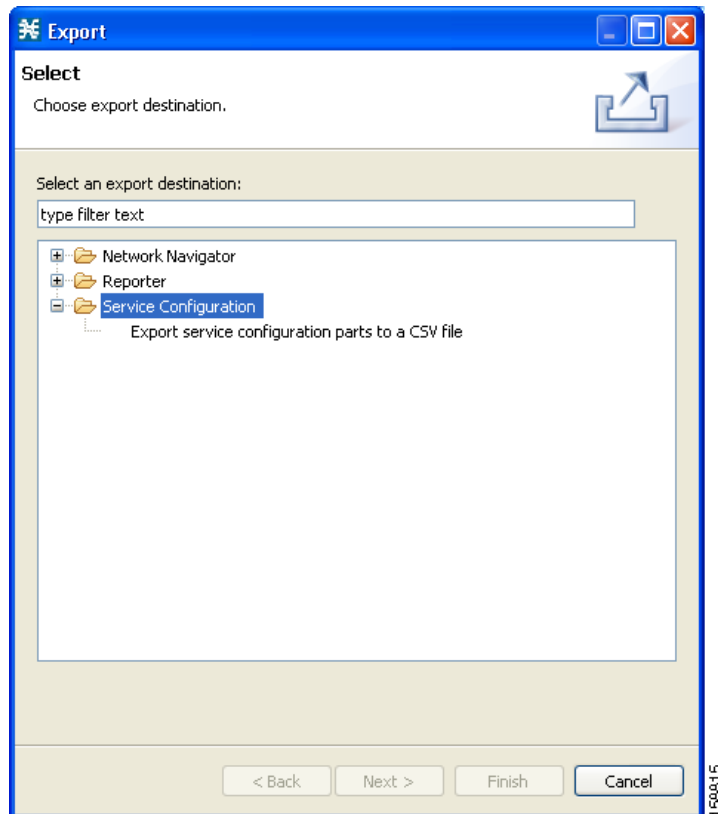
After you add sites and devices to the Network Navigator, you can export this data to a file to back up your settings and to share them with other users, who can import your Network Navigator settings into their Console.

If you use the Site Master Password to store the passwords of the network devices, the passwords are also exported, in encrypted form. This means that other users who import this data need only provide the Site Master Password to access the devices.

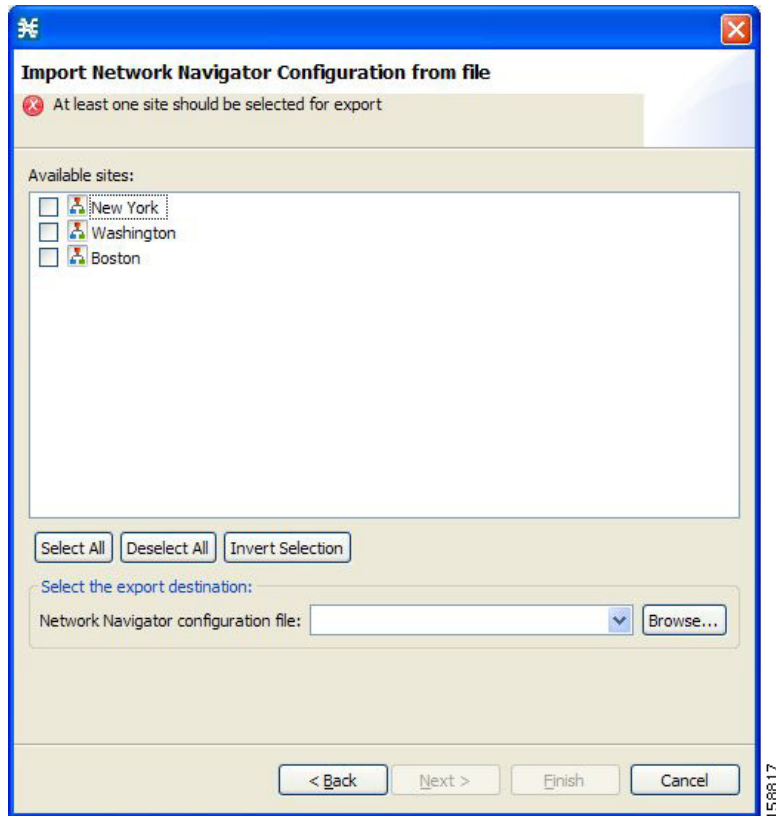
- [How to Export a Network Navigator Configuration, page 5-31](#)
- [How to Import a Network Navigator Configuration, page 5-33](#)

How to Export a Network Navigator Configuration

- Step 1** From the Console main menu, choose **File > Export**.
The Export dialog box appears.



- Step 2** From the export destination list, select **Network Navigator Configuration to a file**.
Step 3 Click **Next**.
The Export Network Navigator Configuration to a file dialog box appears.



The Available sites pane lists all of the sites in the configuration.

Step 4 Select the sites to export, using the check boxes and the select buttons.

Step 5 In the Select the export destination area, click **Browse**.

An Open dialog box appears.

Step 6 Browse to the folder where you want to save the configuration file.

Step 7 In the File name field, enter a new file name, or select an existing *site.xml* file.

Step 8 Click **Open** to select the file.



Note If the file exists, it will be overwritten.

The Open dialog box closes.

Step 9 Click **Finish**.

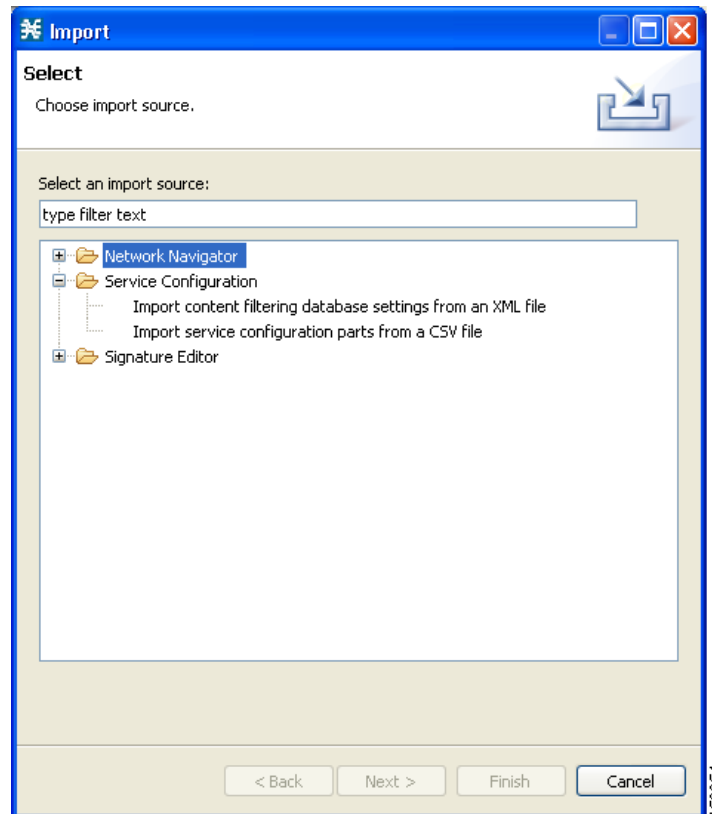
The Export Network Navigator Configuration dialog box closes.

The configuration is saved to the file.

How to Import a Network Navigator Configuration

Step 1 From the Console main menu, choose **File > Import**.

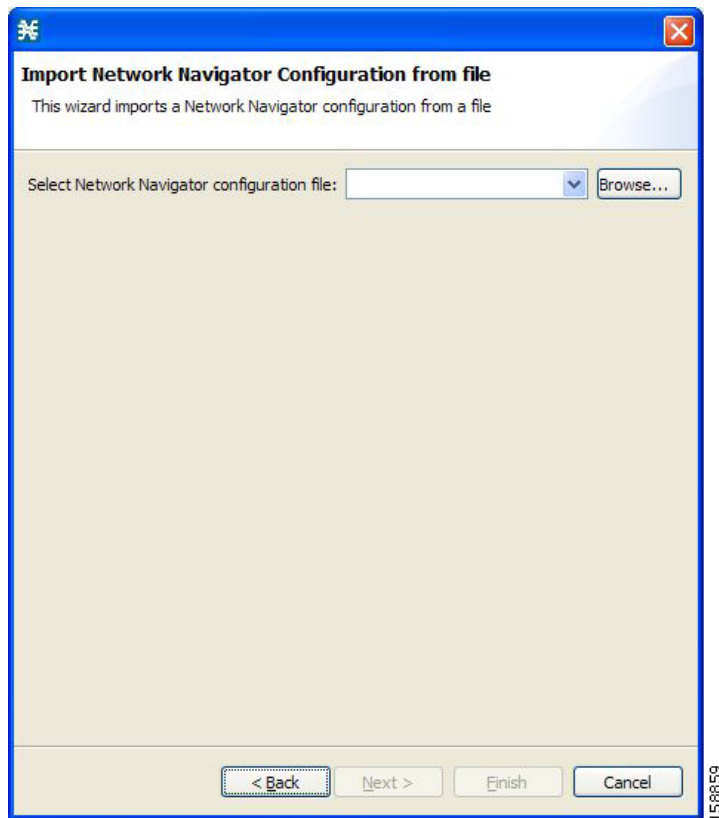
The Import dialog box appears.



Step 2 From the import source list, select **Network Navigator Configuration from file**.

Step 3 Click **Next**.

The Import Network Navigator Configuration from file dialog box appears.



- Step 4** Click **Browse**.
An Open dialog box appears.
- Step 5** Browse to the folder containing the file to import, and select a *site.xml* file.
- Step 6** Click **Open** to select the file.
The Open dialog box closes.
- Step 7** Click **Finish**.
The Import Network Navigator Configuration dialog box closes.
The configuration is imported from the file.

Network Settings Requirements

- [Firewall/NAT Requirements, page 5-35](#)
- [User Authentication, page 5-35](#)
- [How to Disable PRPC Authentication, page 5-36](#)

Firewall/NAT Requirements

The following table lists the firewall/NAT open port settings required for the Network Navigator to operate properly.

Table 5-1 Required Firewall/NAT Settings

Source	Destination	Comments
Workstation	SCE port 14374/TCP	PRPC—Required for all SCE operations
SCE	Workstation port 21/TCP	FTP—Required for the following SCE operations: <ul style="list-style-type: none"> • Install OS • Generate Tech Support Info File
SCE	Workstation ports 21000/TCP to 21010/TCP	FTP—Alternative to port 21/TCP, required if port 21/TCP is already used by another application on the workstation
Workstation	SM port 14374/TCP	PRPC—Required for all SM operations
Workstation	CM port 14375/TCP	PRPC—Required for the CM Online Status operation and for CM authentication

The SCA Reporter may have additional requirements for connecting to the database. For more information, see the *Cisco Service Control Application Reporter User Guide*.

User Authentication

User authentication is performed when a PRPC connection is made to an SCE platform, a CM, or an SM. For authentication to succeed, a PRPC server must be running at the destination, and you must know the username and password of a user of the server.

You define the username and password using the user/password mechanism in the SCE platform or a command-line utility in the SM and CM.

For more information about defining users, see the following:

- SCE—“TACACS+ Authentication, Authorization, and Accounting” in the “Configuring the Management Interface and Security” chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*
- CM—“Managing Users” in the “Managing the Collection Manager” chapter of the *Cisco Service Control Management Suite Collection Manager User Guide*
- SM—“p3rpc Utility” in the “Command-Line Utilities” appendix of the *Cisco Service Control Management Suite Subscriber Manager User Guide*

**Note**

PRPC authentication from the SCA BB Console to any CM/SM/SCE IP address other than the device's real IP address is not supported. This is especially important when the CM/SM/SCE resides on the inside interface of a NATing router or firewall

Workaround:

Redesign your network so that the SCA BB Console is given the real IP address of the CM/SM/SCE. Disable PRPC authentication on the SCE/CM/SM/SCE as described in the following sections.

How to Disable PRPC Authentication

- [How to Disable PRPC Authentication on an SCE Platform, page 5-36](#)
- [How to Disable PRPC Authentication on a CM, page 5-36](#)
- [How to Disable PRPC Authentication on an SM, page 5-36](#)

How to Disable PRPC Authentication on an SCE Platform

Step 1 Use the CLI to disable PRPC authentication.

Run the following CLI in config mode:

```
ip rpc-adapter security-level none
```

How to Disable PRPC Authentication on a CM

Step 1 Edit the CM configuration file.

Edit the *cm/um/config/p3cm.cfg* configuration file:

```
[RPC.Server]
security_level=none
```

Step 2 Reload the CM process.

How to Disable PRPC Authentication on an SM

Step 1 Edit the SM configuration file.

Edit the *~pcube/sm/server/root/config/p3sm.cfg* configuration file:

```
[RPC.Server]
security_level=none
```

Step 2 Load the configuration.

Run the following CLU:

```
p3sm --load-config
```