Cisco Service Control Solution Guide

Cisco Service Control Guide to Upgrading to SCA BB 3.6.x

Revised: February 29, 2012, OL-21070-03

Note This document supports all 3.6.x releases.

1 Overview

Upgrading from Version 3.0.x, 3.1.x, 3.5.x, or 3.6.0 to Version 3.6.5

This guide describes the process of upgrading the Cisco Service Control solution from Version 3.0.x, 3.1.x, 3.5.x, or 3.6.0 to Version 3.6.5. It describes the upgrade process for each of the four components:

- Service Control Application for Broadband (SCA BB)
- Service Control Engine (SCE)
- Subscriber Manager (SM)
- Collection Manager (CM)

The procedure describes a scenario where the Service Control deployment is required to continue functioning throughout the upgrade procedure, with SCE platforms running SCA BB 3.0, SCA BB 3.1, SCA BB 3.5, or SCA BB 3.6 operating concurrently (using the same CM and SM servers).

This procedure aims to minimize service downtime (for however long the upgrade process takes), bound to several limitations, as described in the preceding sections.

Note This is a high level description of the procedure.

Step 1 Upgrade SCA BB:

a. Install the 3.6.5 console.

b. (Optional) Install the SCA BB Service Configuration Utility version 3.6.5, **servconf,** in an empty directory.

Step 2 Upgrade the SM (or SM cluster) according to the procedure described in "Upgrading the Subscriber Manager" section on page 5.

a. Run the SM upgrade script.

The SM does not update an SCE that is identified as standby, even if it is configured as *standalone* in the SM.

Note Only after the SM is configured correctly can you update the SCEs.

Step 3 Deploy a new CM running 3.6.5. See the "Upgrading the Collection Manager" section on page 15.

- In the case of deployment of an additional CM and database for the transition phase (*two CM databases* in total, regardless of whether or not the configuration is bundled), collection works for all SCE platforms (both older versions and 3.6.5). For *non-bundled databases*, there may be several ways to implement this; it is recommended to consult a DB specialist if you are using a non-bundled database.
- Each CM collects RDRs from a single version to a distinct database (either bundled or non-bundled) and CSV repository.

Step 4 Upgrade the SCE platform software using the SCE Software Upgrade Wizard.

- Make sure the upgraded SCE platform RDRs are directed to the CM running version 3.6.0. Service downtime (from a collection perspective) depends on the CM configuration that you have implemented (single or dual during the upgrade).

At this stage, the entire solution is upgraded and fully operational.

Step 5 Remove the second CM running the former version (if one was used) once the upgrade of all SCE platforms is complete.

Supported Working Configurations

The SCA BB release 3.6.5 supports a combination of component versions:

- SCOS 3.6.5
- Application - SCA BB 3.6.5 (PQI for installation on SCE platform)
- SCMS-SM 3.6.5 (if an SM is required for the deployment)
- SCMS-CM 3.6.5 (if a CM is required for the deployment)

Note This document covers the upgrade of a system that includes an SM and a CM. In cases where one or both of these components are not required, the corresponding sections can be ignored.

Rollback Procedure

A software rollback might be required in cases where the upgrade process has failed, or has impaired the service. It requires a downgrade to the previous release to mitigate the damage to the network.

Generally, no automatic downgrade scripts are available for the solution components. To enable downgrade, the older configuration should be backed up before upgrading. To downgrade, a clean installation of the older release is required for each component.

Note When downgrading the SCE, you must first uninstall the SCA BB PQI using the **PQI uninstall file** command. The new PQI file is needed to run this command.

2 Upgrading the SCA BB

This chapter details the procedure for upgrading from a functional SCA BB 3.0.x, SCA BB 3.1.x, SCA BB 3.5.x, or SCA BB 3.6.x deployment to SCA BB 3.6.5.

Upgrading SCA BB

Upgrading SCA BB consists of two steps:

1. Installing the 3.6.5 console. (It is not necessary to uninstall the previous version.)
2. (Optional) Installing the 3.6.5 service configuration utility.

How to Install the Console

Navigate to the Console installation file, *sca-bb-console-3.6.5.exe*, and double-click it.

A standard installation wizard opens. Follow the standard procedure to install the console.

How to Upgrade the SCA BB Service Configuration Utility

Step 1 From the SCA BB installation package, extract the file *scas_bb_util.tgz*, and copy it to a Windows, Solaris, or Linux workstation.

Step 2 Unpack the file to a new folder.

The SCA BB Service Configuration Utility (**servconf**), the SCA BB Real-Time Monitoring Configuration Utility (**rtmcmd**) and associated real-time monitoring report templates, and the SCA BB Signature Configuration Utility (**sigconf**) are located under the bin folder.

3 Upgrading the Subscriber Manager

This chapter describes how to upgrade the Cisco Service Control Management Suite Subscriber Manager (SCMS SM).

Contents of the Distribution Files

The SCMS SM components are supplied in three distribution files:

- SM for Solaris
- SM for Linux
- Login Event Generators (LEGs)

Each distribution file is supplied as a tar file, which is compressed by gzip and has an extension of **.tar.gz**. For details see the Installing and Upgrading chapter of *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Upgrading the Subscriber Manager

The Subscriber Manager supports several types of upgrade procedures, according to the SM version that was previously installed and the requirement (or lack of requirement) for fail-over in the new installation.

There are three types of upgrade procedure:

- How to Upgrade a Standalone Setup, page 7
- How to Upgrade a Standalone Setup to a Cluster Setup, page 8
- How to Upgrade a Cluster Setup, page 9

Data Duplication Procedure

The data duplication procedure enables the user to duplicate or copy the entire database from one machine to the other, and then keep the databases synchronized by running the replication agent at the end. Some of the upgrade procedures use this procedure.

For details of the procedure, see the Database Duplication Recovery section of *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Automatic Upgrade of Subscribers with VLAN Mappings

VLAN mappings are related to VPN rather than to a subscriber. During the upgrade procedure, the SM automatically creates a VPN with the VLAN-ID of the subscriber and associates a subscriber with the full range IP mapping to the new VPN.

For example, subscriber *sub1* with VLAN-ID=15 results in the creation of VPN 15 with VLAN-ID=15 and subscriber *sub1* with the mapping 0.0.0.0/0@VLAN-ID.

Automatic Upgrade of RADIUS Listener

During the upgrade procedure, the SM modifies the RADIUS sections in the configuration file according to the following rules:

- The **radius_attribute** and **radius_attribute_type** properties are moved to a new section.
- A new field property is added to replace the **radius_attribute** and **radius_attribute_type** properties.
- The **strip_type=remove_suffix** property is replaced with **field_manipulation.<field name>=(.*)<strip_character >.*.**
- The **strip_type=remove_prefix** property is replaced with **field_manipulation.<field name>=.*<strip_character >(.*).**
- The **use_default** property and default value are replaced with **mapping_table.^$=<default>.**
- The **radius_attribute_vendor_id** and **radius_sub_attribute** properties are replaced with the format **radius_attribute.**

Configuring the Required Memory Settings

To prepare the SM for the upgrade, configure the system kernel configuration file on the SM.

TimesTen requires that certain changes be made in the operating system kernel configuration file:

- For Solaris, modify file **/etc/system**.
- For Linux, modify file **/etc/sysctl.conf**.

These changes increase the shared memory and semaphore resources on Solaris machines from their defaults. For additional information regarding these changes, refer to the *TimesTen* documentation.

Note It is recommended that you review the **/etc/system** or the **/etc/sysctl.conf** file before running the **tt-sysconf.sh** script, because the script overwrites the current file settings with the values listed in the *To make the required changes manually* procedure. If you want to keep some or all of the current file settings, edit the system configuration file and perform the changes manually.

You can make the changes automatically or manually.

- To make the required changes automatically, run the **tt-sysconf.sh** script.

  The root user must invoke this script file, without arguments, as follows:

  ```
  # tt-sysconf.sh
  ```

- To make the required changes manually:

Note Editing the configuration file manually is required when you require support for more than 100,000 subscribers in the SM. Your system's sizing requirements only affect the shared memory size. To determine the correct configuration values for your system, see Table 4-6 through Table 4-9 in the "Installation and Upgrading" chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

  – For Solaris, make the required changes manually by adding the following lines to the **/etc/system** file and configuring the shared memory size:

  ```
  *---- Begin settings for TimesTen
  set semsys:seminfo_semmni = 20
  set semsys:seminfo_semmsl = 100
  set semsys:seminfo_semmns = 2000
  set semsys:seminfo_semmnu = 2000
  set shmsys:shminfo_shmmax = 0x20000000
  *---- End of settings for TimesTen
  ```

  – For Linux, make the required changes manually by adding the following lines to the **/etc/sysctl.conf** file and configuring the shared memory size:

  ```
  *---- Begin settings for TimesTen
  kernel.shmmax = 536870912
  kernel.sem = 250 32000 100 100
  *---- End of settings for TimesTen
  ```

How to Upgrade a Standalone Setup

This upgrade procedure requires service down-time.

Note For the upgrade procedure from a standalone setup to a cluster setup, see "How to Upgrade a Standalone Setup to a Cluster Setup" section on page 8.

Step 1 Extract the distribution files.

Before you can upgrade the SM, you must first load and extract the distribution files on the installed machine or in a directory that is mounted to the installed machine.

a. Download the distribution files from the Cisco.com.

b. Use an FTP to load the distribution files to the SM.

c. Unzip the files using the **gunzip** command.

```
gunzip SM_dist_<version>_B<build number>.tar.gz
```

d. Extract the tar the file using the **tar** command.

```
tar -xvf SM_dist_<version>_B<build number>.tar
```

Step 2 Edit the **install-def-cfg** file.

Edit the **install-def.cfg** configuration file and set the **PermSize** and **TempSize** parameters according to the recommendations described in Appendix A. For further information, see "Configuring the Required Memory Settings" section on page 6.

Step 3 Run the **upgrade-sm.sh** script.

To upgrade from non-cluster setups, the SM distribution provides an upgrade script that implements an upgrade from previous versions. The upgrade procedure script preserves the subscriber database and the entire SM configuration, including network elements, domains, and application-specific components.

Note For Solaris: Previous versions of the SM on Solaris used a 32-bit or 64-bit Java Virtual Machine (JVM) and database. The SM is currently installed with a 64-bit JVM and database. There is no choice as to whether to upgrade to 64-bit.

Note For Linux: The Linux platform is used only with a 32-bit JVM and database.

Note It is not possible to run the script if the **/etc/motd** file exists. The file should be moved or removed prior to running the **upgrade-sm.sh** script.

From your workstation shell prompt, run the **upgrade-sm.sh** script.

```
# upgrade-sm.sh
```

Step 4 Add a user for PRPC authentication.

If upgrading from a version of the SM prior to 3.0.5, it is necessary to add a user for PRPC authentication because SCA BB requires a username and password when connecting to the SM.

To add a user for PRPC authentication, use the **p3rpc** CLU. For example:

```
>p3rpc --set-user --username=username --password=password
```

Step 5 Configure the SCE platforms.

If using a cascade SCE setup, configure the cascade SCE pair in the **p3sm.cfg** file as described in the SCE.XXX section in the Configuration File Options appendix of *Cisco Service Control Management Suite Subscriber Manager User Guide*.

How to Upgrade a Standalone Setup to a Cluster Setup

This section describes the basic procedure for upgrading from a standalone setup to a cluster setup. This upgrade procedure requires service down-time.

Note This procedure attempts to minimize the SM downtime as much as possible. Therefore, if subscriber service is not an issue, use the procedure for installing a new machine and upgrading a new machine instead.

In the following procedure, SM-A is the original SM machine and SM-B is the new SM machine being added for redundancy.

Step 1 Install the VCS on both machines.

Step 2 Install SM-B.

To install SM-B, follow the procedure described in the Installing the Subscriber Manager section of *Cisco Service Control Product Installation Guide*.

Step 3 Upgrade SM-A.

To upgrade SM-A, follow the procedure described in How to Upgrade a Standalone Setup, page 7.

Note From this step until the upgrade procedure is completed, there is no SM to handle subscribers.

Step 4 Replicate the SM configuration from SM-A to SM-B (copy all the configuration files from the ~pcube/sm/server/root/config folder).

Copy the **p3sm.cfg** configuration file manually from SM-A to SM-B and load the configuration file using the following CLU command:

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

Step 5 Duplicate the subscriber database.

See the "Data Duplication Procedure" section on page 5 for the data duplication procedure.

Configure the replication scheme for the data store replication to the redundant machine.

Note This CLU must be run on both machines, with user as **pcube**.

```
>p3db --set-rep-scheme
```

Step 6 Create a cluster.

a. Configure both SM-A and SM-B to support a cluster.

On each machine, open the **p3sm.cfg** configuration file in any standard text editor and in the **[SM High Availability Setup]** section, set `topology=cluster`.

Load the updated configuration file using the following CLU command:

p3sm --load-config

b. Make SM-B standby.

Use the CLU command **p3cluster --standby**.

c. Ensure that SM-A is active.

   Use the CLU command **p3cluster --active**.

d. Configure the VCS.

e. Run the VCS on the setup.

Step 7 Configure the LEG applications to send logins to the cluster virtual IP.

How to Upgrade a Cluster Setup

This section describes the procedure for upgrading from a cluster setup to a cluster setup without a service downtime. This section contains the following subsections:

Before You Start

- Identify the devices in the cluster setup.
- Understand the Java Virtual Machine (JVM) used by the Cisco SCMS Subscriber Manager on your operating system:
  - Versions prior to 3.6.x of the Cisco SCMS Subscriber Manager on Solaris used a 32-bit or 64-bit JVM and database. From Subscriber Manager Version 3.0.3, the Subscriber Manager is installed with a 64-bit JVM and database. There is no choice as to whether to upgrade to 64-bit JVM.
  - The Linux platform is used only with a 32-bit JVM and database.
- Understand how to download and extract the distribution files. For details, see the "Downloading and Extracting the Distribution Files" section on page 9.
- Understand the scripts used while upgrading a cluster setup. For details, see the "Understanding the Scripts Used During Upgrade" section on page 9.

Downloading and Extracting the Distribution Files

Before you upgrade the Subscriber Manager, you must download and extract the distribution files on the installed machine or in a directory that is mounted to the installed machine.

Step 1 Download the distribution files from Cisco.com.

Step 2 Use an FTP to load the distribution files to the Subscriber Manager.

Step 3 Unzip the files by using the **gunzip** command:

```
gunzip SM_dist_<version>_B<build number>.tar.gz
```

Step 4 Extract the tar file using the **tar** command:

```
tar -xvf SM_dist_<version>_B<build number>.tar
```

Understanding the Scripts Used During Upgrade

During the process of upgrading a cluster, you might use the following scripts:

- cluster-upgrade.sh. For details, see the "Understanding the cluster-upgrade.sh script" section on page 9.
- install-vcs-agents.sh. For details, see the "Understanding the install-vcs-agents.sh script" section on page 10.

Understanding the cluster-upgrade.sh script

Use this script, which is provided with the Subscriber Manager, to upgrade a cluster setup with earlier versions of Cisco SCMS Subscriber Manager to a cluster setup with the latest version of the Cisco SCMS Subscriber Manager.

The cluster-upgrade.sh script preserves the subscriber database and the entire Subscriber Manager configuration, including network elements, domains, and application-specific components.

The script performs the following actions:

- Detects the current Subscriber Manager version.
- Detects the new version of the Subscriber Manager.
- Verifies whether Java is installed on the machine.
- Verifies whether the user **pcube** exists.
- Verifies whether Subscriber Manager Version 3.x or later is present on the system.
- Verifies the values, if any, configured in **install-def.cfg**.
- Stops the Subscriber Manager, if it is running.
- Backs up the contents in the subscriber database to an external file.
- Removes the Subscriber Manager database.
- Backs up the Subscriber Manager configuration files.
- Installs the updated version of the Subscriber Manager and the Subscriber Manager Database.
- Invokes a separate program for upgrading the Subscriber Manager and the database configuration files.
- Restores the contents of the subscriber database that were backed up.
- When activated on the second machine, the script copies the contents of the database from the currently active Subscriber Manager; because the currently active Subscriber Manager contains the latest data.

You do not have to start the Subscriber Manager after running the script.

Table 1 lists the command options for the cluster-upgrade.sh script.

Table 1 Command options for cluster-upgrade.sh

Options	Description
`-h`	Use this option to see the details on how to use the command options.
`-1`	Use this option when activating the script on the first machine.
`-2`	Use this option when activating the script on the second machine.

Understanding the install-vcs-agents.sh script

For details about the install-vcs-agents.sh script, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Upgrading a Cluster Setup

To upgrade a cluster setup, complete the following steps:

Step No.	Action	Notes
Step 1	Configure the system kernel configuration file on both the machines: **a.** Configure the system kernel configuration file on the standby Subscriber Manager. **b.** Reboot the standby SM. **c.** Manually trigger a failover by using the Veritas Cluster Manager and wait until the standby SM becomes active and the active SM shifts to the standby SM. **d.** Run the following VCS CLU command from /opt/VRTSvcs/bin: `# hagrp -switch service group name to System` **e.** Repeat Step a. and Step b. on the new standby Subscriber Manager.	Before starting the upgrade procedure, configure the system kernel configuration file on both the machines. For details about the system kernel configuration procedure, see the "Configuring the Required Memory Settings" section on page 6.
Step 2	Extract the distribution files on both the machines.	For details about downloading and extracting the distribution files, see the "Downloading and Extracting the Distribution Files" section on page 9.
Step 3	Stop VCS monitoring on the standby machine: **a.** Log in as the *root* user. **b.** Use the following VCS CLU command from /opt/VRTSvcs/bin to stop VCS monitoring of the Subscriber Manager: `#./hastop -local`	—
Step 4	Edit the install-def.cfg file on both the machines and set the PermSize and TempSize parameters according to the recommendations described in "Configuring the Required Memory Settings" section on page 6.	For details about the required memory settings, see the *Cisco Service Control Product Installation Guide*.
Step 5	Pause database replication on the active machine: **a.** On the active machine, change the directory to the location where you extracted the distribution files. **b.** Run the p3db --rep-pause CLU command from the scripts directory. **c.** Run the p3db --rep-status CLU command from the scripts directory and verify that replication is in *pause* state. **d.** Return to the standby machine.	This step is applicable only when upgrading the first Subscriber Manager machine.
Step 6	Run the cluster-upgrade.sh script on the standby machine: `# cluster-upgrade.sh [command-options]` Do not start the SM after running cluster-upgrade.sh.	For details about the cluster-upgrade.sh script, see the "Understanding the Scripts Used During Upgrade" section on page 9
Step 7	Wait until the cluster-upgrade.sh script finishes all tasks.	—

Step No.	Action	Notes

Step 8	Stop the replication and start the SM on the standby machine.
	The following steps should be performed *only when performing upgrade on the first machine*.
	a. Stop the SM replication:
	`# ./p3db --rep-stop`
	b. Start the SM:
	`# ./p3sm --start --wait`
	c. Use the **p3sm** CLU command to verify the status of the SM.
	`-bash-3.1$ p3sm --sm-status`
		Because the database schema was changed, there is a need to load the SM for the first time without replicating the changes to the standby machine.
		The SM boot time after the upgrade will be longer than usual due to the extra time taken to initialize the database indexes.
		If the SMS-STATUS indicates a failure, *stop the upgrade*. For details on troubleshooting the SM in failure mode, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Step 9	Run the **install-vcs-agents.sh** script on the standby machine: **`# install-vcs-agents.sh`** [*command-options*]	—
Step 10	Restart VCS monitoring on the standby machine: **a.** Run the following VCS CLU command from /opt/VRTSvcs/bin: `#./hastart` VCS monitoring starts the SM process automatically in the initialization state. **b.** Use the **p3sm** CLU command to check whether the SM is up: **`-bash-3.1$ p3sm --sm-status`** **c.** Use the **p3cluster** CLU command to set the SM to the standby state: **`-bash-3.1$ p3cluster --standby`**	The **./hastart** command starts the replication agent that updates the database schema on the active machine. After this operation is performed, you cannot downgrade to an earlier version.
Step 11	Continue database replication on the active machine: **a.** On the *Active* machine, change the directory to the location where you extracted the distribution files. **b.** Run the **scripts/p3db --rep-continue** CLU command. **c.** Run the **~pcube/sm/server/bin/p3db --rep-status** CLU command and verify that replication is in the *start* state. **d.** Return to the standby workstation.	This step is applicable only when upgrading the first machine and only if Step 5 was performed.

Step 12	Verify that the changed data has been replicated.
	Wait until the replication of all the data that was changed while the upgrade script was running.
	• On the active Subscriber Manager add a dummy subscriber using the **p3subs** CLU:
	`-bash-3.1$ p3subs --add -s dummySub`
	• On the standby Subscriber Manager, login as *root* user, and run the verify-subscriber.sh script:
	`#./verify-subscriber.sh dummySub`
		When upgrading the second Subscriber Manager, add a subscriber with a name other than *dummySub* because you have already added a subscriber with this name while upgrading the first Subscriber Manager.

Step No.	Action	Notes
Step 13	(Optional) Install the MPLS/VPN BGP LEG.	For more information, see the *Cisco SCMS SM LEGs User Guide*.
Step 14	Manually trigger a failover using the Veritas Cluster Manager and wait until the standby SM becomes active and the active SM becomes the standby: Run the following VCS CLU command from /opt/VRTSvcs/bin: `# hagrp -switch service group name -to System`	For more information about the **hagrp** CLU command, refer to your Veritas Cluster Server documentation. After performing the manual failover, the standby SM on which you perform the upgrade procedure becomes the active SM. The previously active SM becomes the new standby SM.
Step 15	Repeat the upgrade procedure on the standby SM. To upgrade the second SM, repeat the procedure from Step 2 . But, do not perform Step 5, Step 8, and Step 11.	—

Step 16	Upgrade the database replication protocol version:
	a. Stop VCS monitoring of the standby SM.
	Use the following VCS CLU command from /opt/VRTSvcs/bin:
	`#./hastop -local`
	b. Change the replication protocol.
	On the standby SM, run the following CLU command:
	`# p3db --upgrade-rep-protocol`
	c. Restart VCS monitoring.
	From the /opt/VRTSvcs/bin folder, run the following VCS CLU command:
	`#./hastart`
	VCS monitoring starts the SM process automatically in the initialization state.
	d. Use the **p3cluster** CLU command to set the SM to the standby state:
	`-bash-3.1$ p3cluster --standby`
	e. Manually trigger a failover using the Veritas Cluster Manager and wait until the standby SM becomes active and the active SM becomes the standby one.
	f. Run the following VCS CLU command from /opt/VRTSvcs/bin:
	`# hagrp -switch service group name -to System`
	g. Repeat Step a. to Step f. on the new standby SM.
		Perform this operation after both the SMs are upgraded.
		Run the commands described in this step as the *admin* user on *both* the machines to upgrade the database replication protocol version.
		The **p3db --upgrade-rep-protocol** CLU command performs the following actions:
		• Removes the DB security flag
		• Stops the SM
		• Restarts the DB daemon
		• Starts the SM
		• Starts SM replication
		For more information about the **hagrp** command, refer to your Veritas Cluster Server documentation.

Step No.	Action	Notes
Step 17	Add a user for PRPC authentication using the **p3rpc** CLU, for example: **-bash-3.1$ p3rpc --set-user --username**=*username* **--password**=*password* **--remote**=*OTHER_SM_IP[:port]*	If you are upgrading from a version of the SM prior to Version 3.0.5, it is necessary to add a user for PRPC authentication because Cisco SCA BB requires a username and password to connect to the SM.
Step 18	Configure the Cisco SCE platforms.	If you have a cascade SCE setup, configure the cascade SCE pair in the p3sm.cfg file. For details, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.
Step 19	Remove the dummy subscribers. On the new active SM, run the following CLU: **-bash-3.1$ p3subs --remove -subscriber**=first dummy subscriber name **-bash-3.1$ p3subs --remove -subscriber**=second dummy subscriber name	After successfully upgrading both the SMs we recommend that you remove the dummy subscribers that were added in order to verify replication during the upgrade.

How to Downgrade the Subscriber Manager

This section describes the procedure to downgrade the SM to a previous version.

Step 1 Perform the uninstall procedure described in the Installing and Upgrading chapter, the How to Uninstall the Subscriber Manager section of *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Step 2 Perform the installation procedure described in the Installing the Subscriber Manager section of *Cisco Service Control Product Installation Guide*.

Note The **upgrade-sm.sh** and **cluster-upgrade.sh** upgrade scripts do not support SM downgrade.

4 Upgrading the Collection Manager

This chapter describes the procedures for upgrading the CM.

When upgrading a complete system, it is recommended to install a second CM running the new version and then simply uninstall the CM running the previous version, thereby providing a seamless transition to the new version. In this case, no upgrade procedure is run on the CM.

To install the CM, see the Installing the Collection Manager section of *Cisco Service Control Product Installation Guide*.

How to Upgrade the Collection Manager to Version 3.6.5

Step 1 Get the CM software as described in *Cisco Service Control Management Suite Collection Manager Quick Start Guide*.

Step 2 Change the directory to **install-scripts** under the distribution kit root.

Step 3 As the scmscm user, stop the CM server.

```
$ ~scmscm/cm/bin/cm stop
```

Step 4 As the root user, run the **install-cm.sh** script.

```
# ./install-cm.sh -o
```

Step 5 As the scmscm user, start the CM server.

```
$ ~scmscm/cm/bin/cm start
```

Note If you upgrade from version 3.0.5 or 3.0.6, the PRPC users file is deleted. You must log in to the CM and redefine the PRPC users.

Verifying that the Server is Operational

To verify that the server is functioning correctly, use the **alive.sh** script:

```
~scmscm/setup/alive.sh
```

The script verifies that the following components are operational:

- Collection Manager
- Database (in the bundled database case)
- Report tables (in the bundled database case)

If any component is down, the script issues an error message.

As the scmscm user, run the **alive.sh** script

Note It takes time for the components to initialize after a startup; after a restart, wait five minutes before running this script.

5 Upgrading the SCE Platform Software

This chapter describes the wizard that upgrades the SCE platform software.

The console SCE Software Upgrade Wizard performs a software upgrade on one or more SCE platforms. The wizard allows you to select the following:

- SCE platforms to be upgraded
- Firmware (pkg) version to upgrade to
- Application (pqi) version to upgrade to
- Service configuration (pqb) to apply
- Protocol pack (spqi) to apply

Before You Start

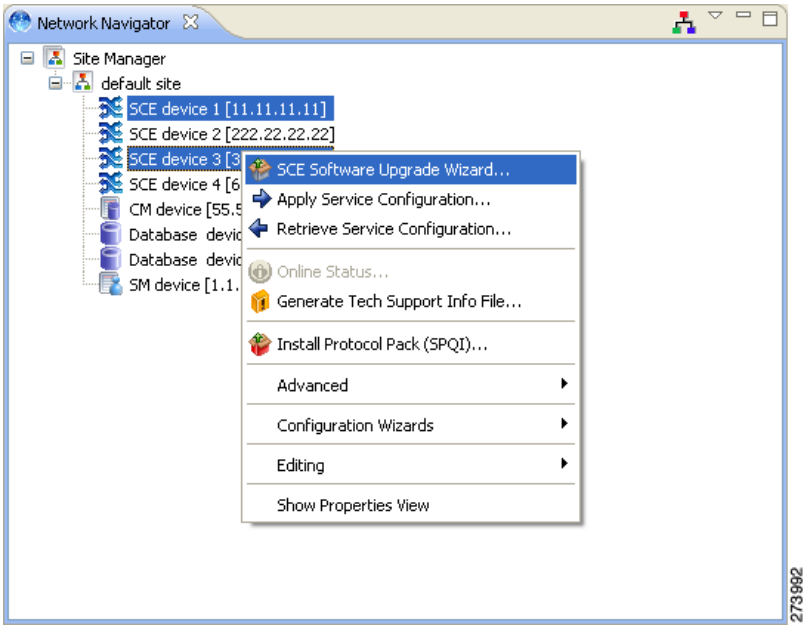
Before you begin the SCE platform upgrade, make sure you do the following:

- Gather the IP addresses of all SCE platforms to be upgraded. (Not necessary if they are all defined in the Network Navigator)
- Download the relevant pkg file, pqi file, and protocol pack to a local location or to a location accessible by FTP. If using an FTP site, make sure to have the complete FTP location and path for each file.
- Decide what service configuration to use:
  - *Default service configuration*—creates a default pqb file and applies to each SCE platform.
  - *Current service configuration*—retrieves the current service configuration before the upgrade and then re-applies after the upgrade is complete.
  - *Other*—specify the desired pqb file to be applied.

How to Upgrade the SCE Platform Software

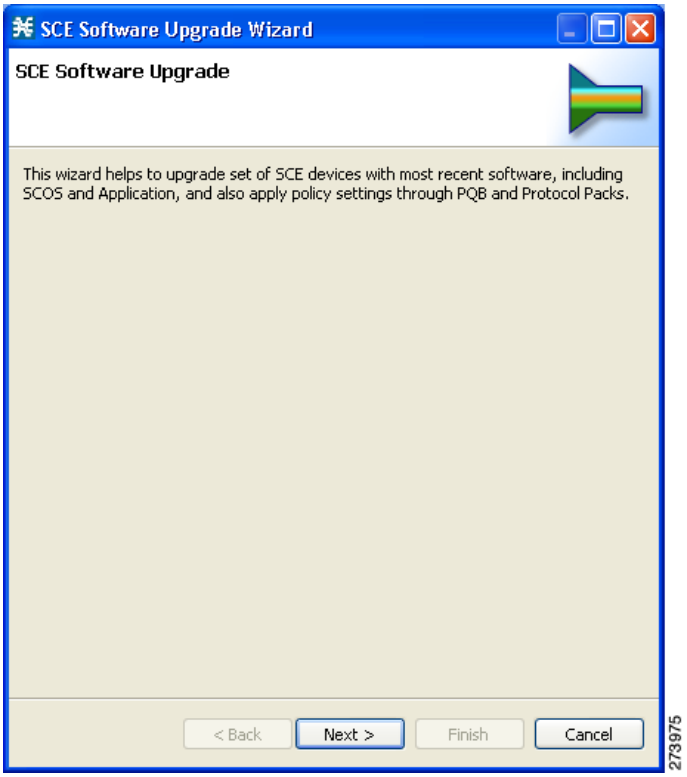
Step 1 In the Network Navigator of the console, select the SCE platforms to be upgraded. Right-click and select **SCE Software Upgrade Wizard** from the menu (see Figure 1).

Figure 1 Network Navigator Window



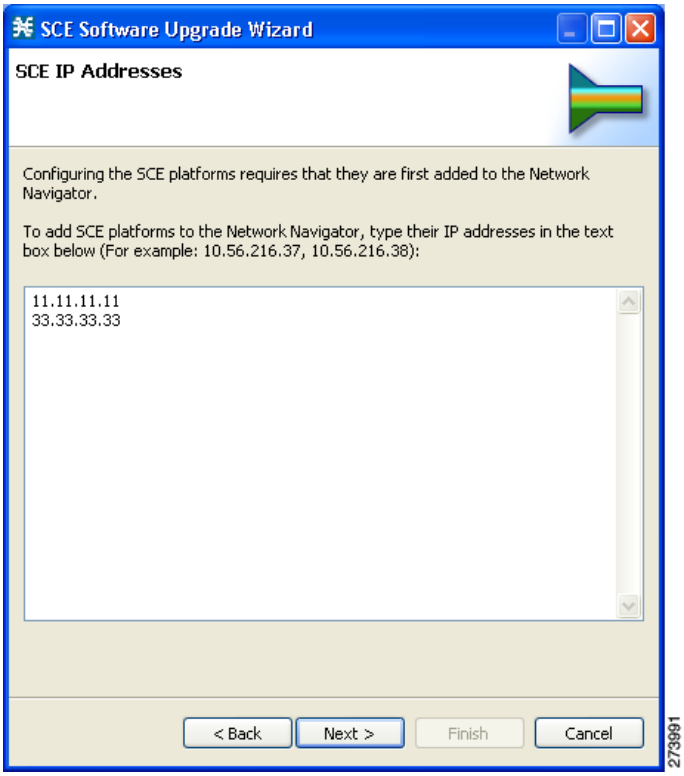
The SCE Software Upgrade Wizard opens (see Figure 2).

Figure 2 SCE Software Upgrade Wizard—SCE Software Upgrade Window



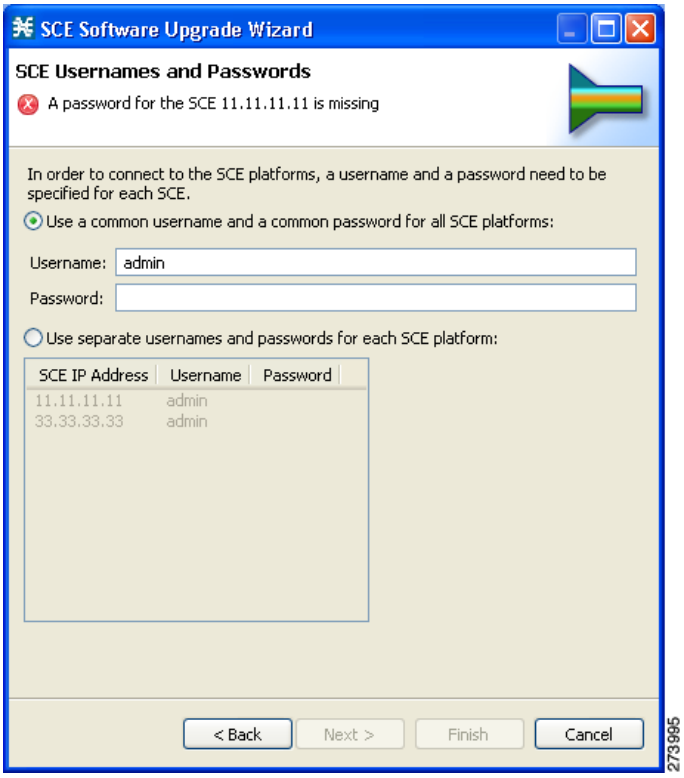
Step 2 In the SCE IP Addresses window, verify that the IP addresses of all the SCE platforms to be upgraded appear. If none appears, add them in (see Figure 3).

Figure 3 SCE Software Upgrade Wizard—SCE IP Addresses Window



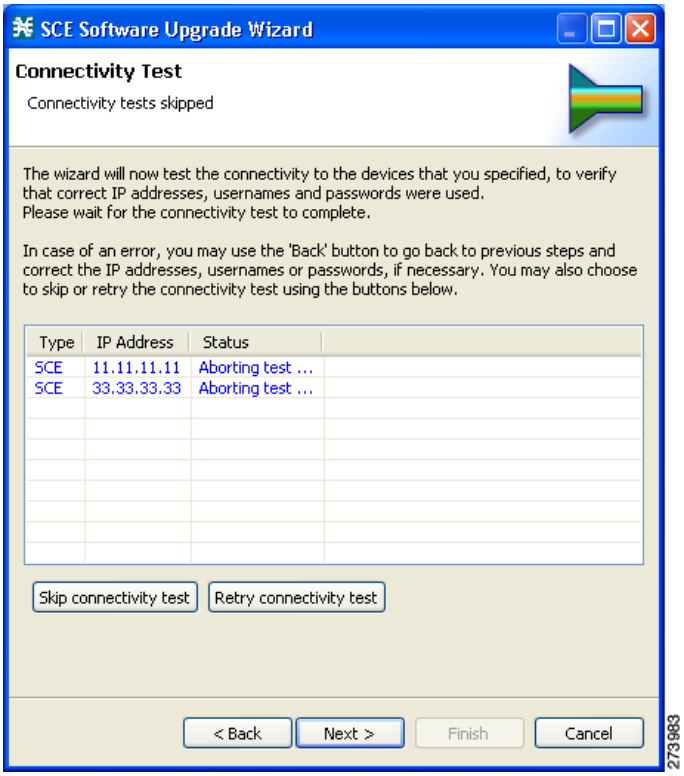
Step 3 In the SCE Username and Password window, enter the username and password required to access the SCE platform. You may use the same username and password for all the platforms or enter a different username and password for each platform (see Figure 4).

Figure 4 SCE Software Upgrade Wizard—SCE Usernames and Passwords Window



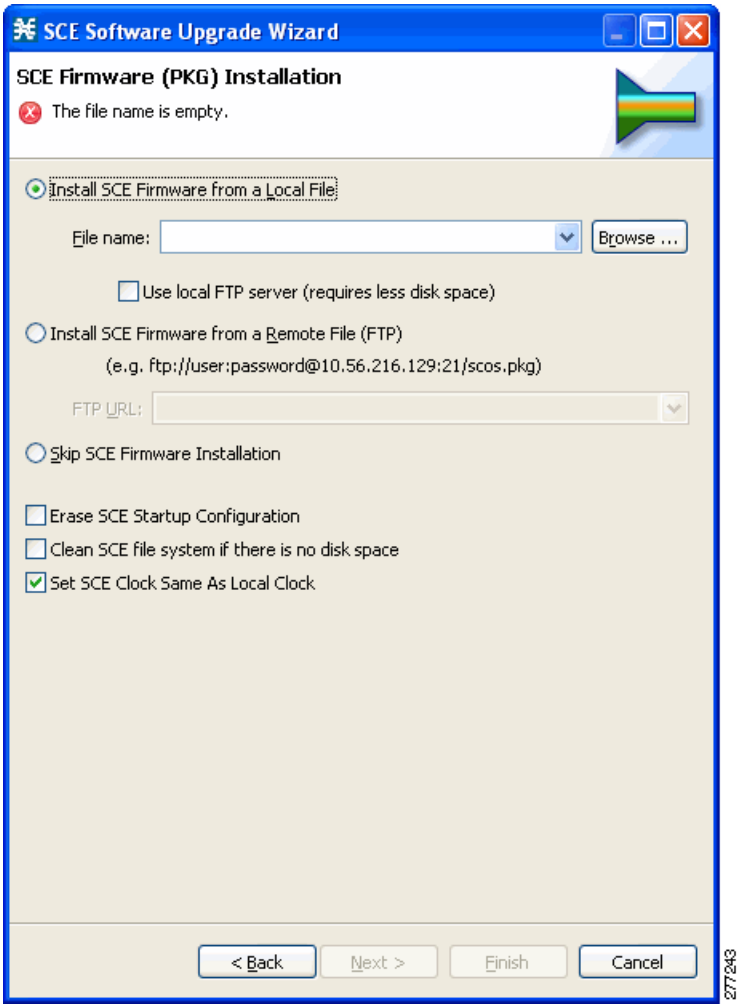
Step 4 The Connectivity Test window (see Figure 5) shows the attempt results to connect to all the SCE platforms on the list. This step verifies that all SCE platforms can be connected to for upgrade.

Figure 5 SCE Software Upgrade Wizard—Connectivity Test Window



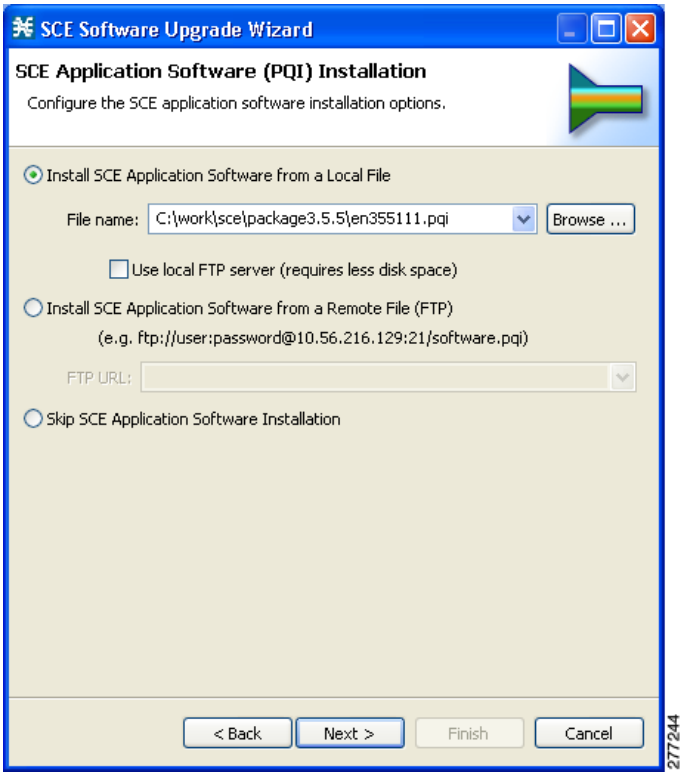
Step 5 In the SCE Firmware (PKG) Installation window (see Figure 6), specify the location of the PKG file to be installed on all the selected SCE platforms.

Figure 6 SCE Software Upgrade Wizard—SCE Firmware (PKG) Installation Window



Step 6 In the SCE Application Software (PQI) Installation window (see Figure 7), specify the location of the pqi file to be installed on all the selected SCE platforms.

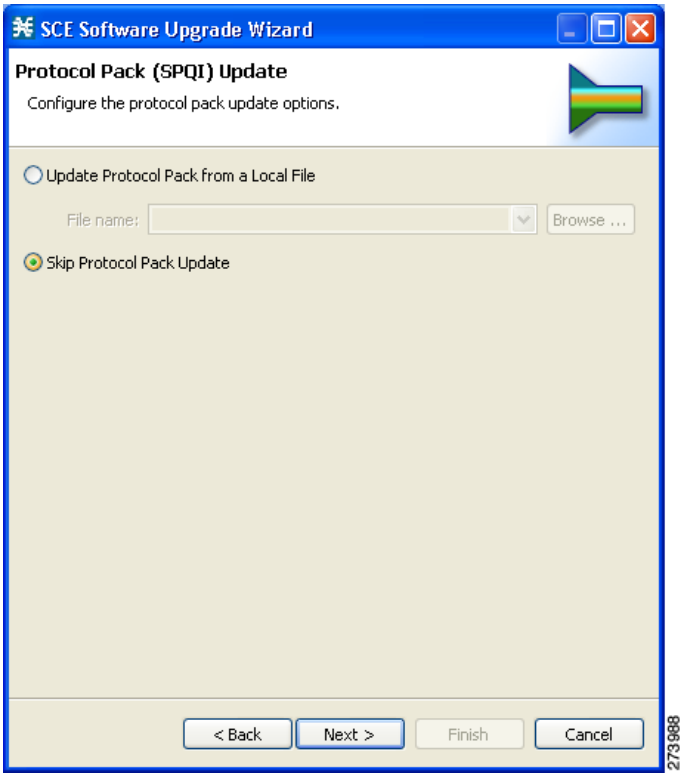
Figure 7 SCE Software Upgrade Wizard—SCE Application Software (PQI) Installation Window



Step 7 In the Protocol Pack (SPQI) Update window (see Figure 8), specify the location of the protocol pack to be installed on all the selected SCE platforms.

Note The version of the Protocol Pack you install during the upgrade must be greater than or equal to that of the Protocol Pack you are upgrading from.

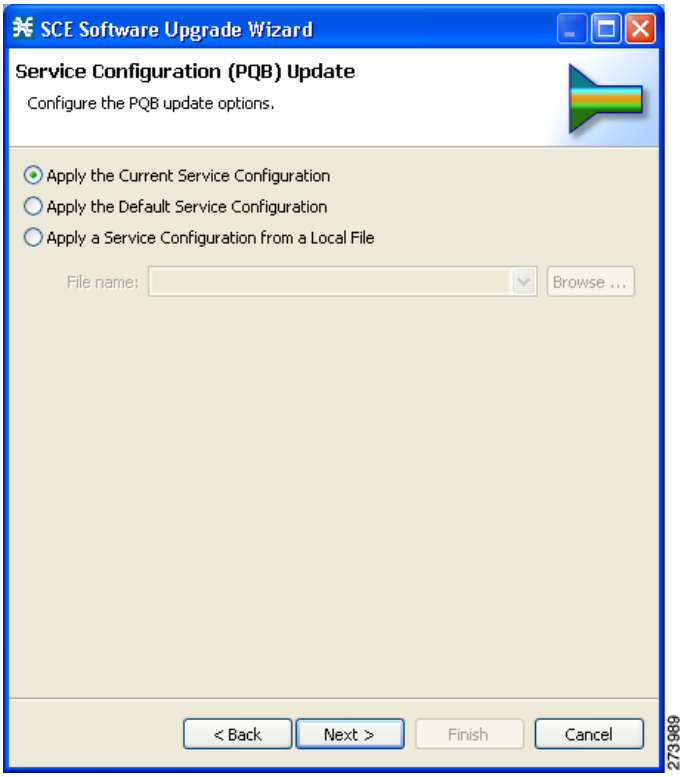
Figure 8 SCE Software Upgrade Wizard—Protocol Pack (SPQI) Update Window



Step 8 In the Service Configuration (PQB) Update window (see Figure 9), select the service configuration to be applied to the SCE platforms:

- Current service configuration: the current service configuration is retrieved before the software upgrade and then re-applied after the upgrade is complete.
- Default service configuration: a default pqb file is created and applied to each SCE platform.
- Other: specify the desired pqb file to be applied.

Figure 9 SCE Software Upgrade Wizard—Service Configuration (PQB) Update Window



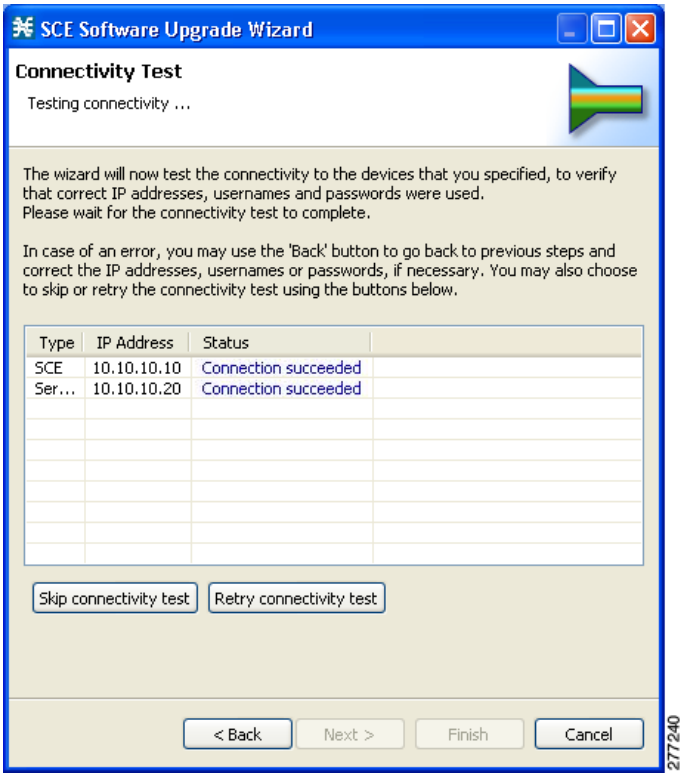
Step 9 Click **Next**.

The Connectivity Test window of the SCE Software Upgrade window opens (see).

The connectivity test verifies the connections to the defined devices.

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 connectivity test**. The connections are validated when you click **Finish** at the end of the wizard.

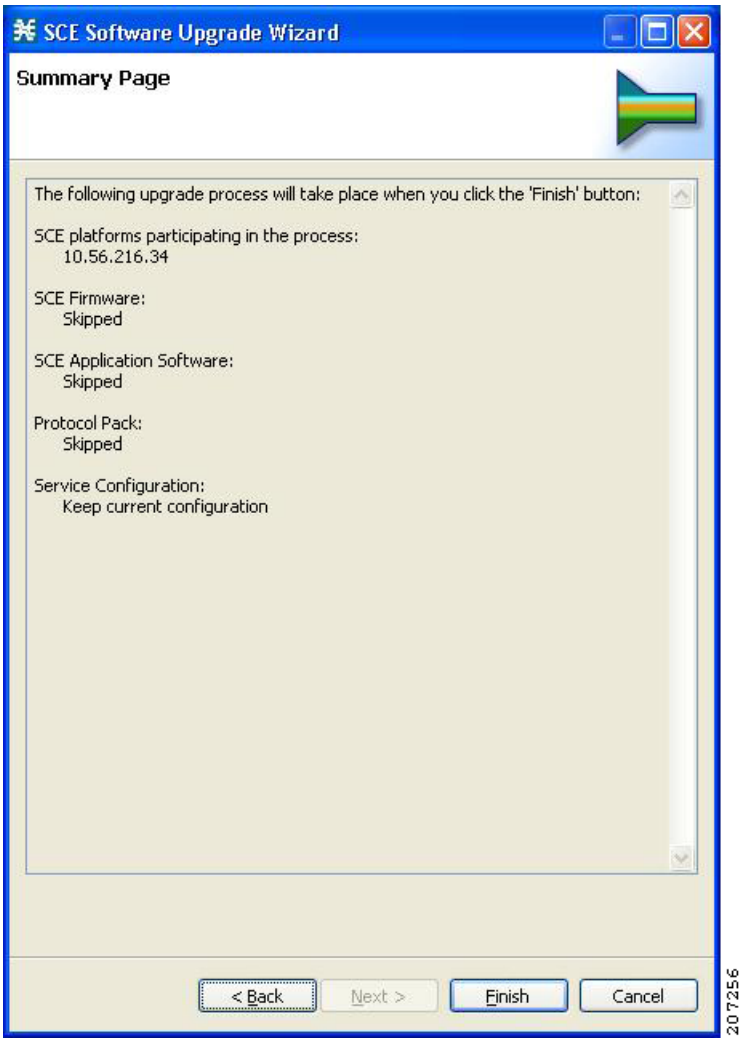
Figure 10 Connectivity Test



Step 10 Summary Page summarizes all the information (see Figure 11). Verify that all the IP addresses and file locations are correct.

- Click **Back** to edit any information.
- Click **Finish** to begin the upgrade process as specified.

Figure 11 SCE Software Upgrade Wizard—Summary Window



This system checks the following:

- The specified SCE platforms can be located by supplied IP addresses.
- If the PKG and/or PQI files are located at the remote FTP server, its availability is verified.
- Supplied credentials are valid for all SCE platforms.
- Specified PKG, PQI, PP, and PQB versions comply.

  If the user requested that any of these components not be upgraded (selected **Skip** for any file), the version of those files are retrieved from SCE platform for this verification. For instance, if the user requested to skip PKG installation and install PQI version 3.6.0, version information about the currently installed PKG file is retrieved. (If this is SCOS 3.1.5, an error is reported.)

A list of all problems and errors is displayed when the verification process is complete.

The basic steps being performed during the upgrade are as follows (assuming all components are upgraded):

- Retrieve the current service configuration from the SCE platform (only if the current service configuration is going to be re-installed after the upgrade).

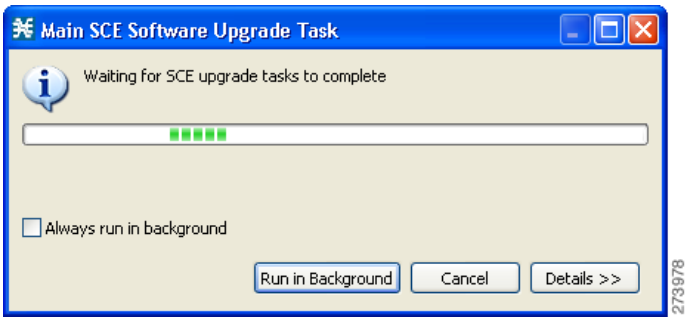
- Uninstall the existing application software (PQI).
- Upgrade SCE platform firmware (PKG).
- Install application software (PQI).
- Apply service configuration (PQB).
- Install the protocol pack (SPQI).

The specified SCE platforms are upgraded simultaneously, with the upgrade process for each SCE platform running in separate thread.

Step 11 The system keeps you informed of the progress of the upgrade (see Figure 12).

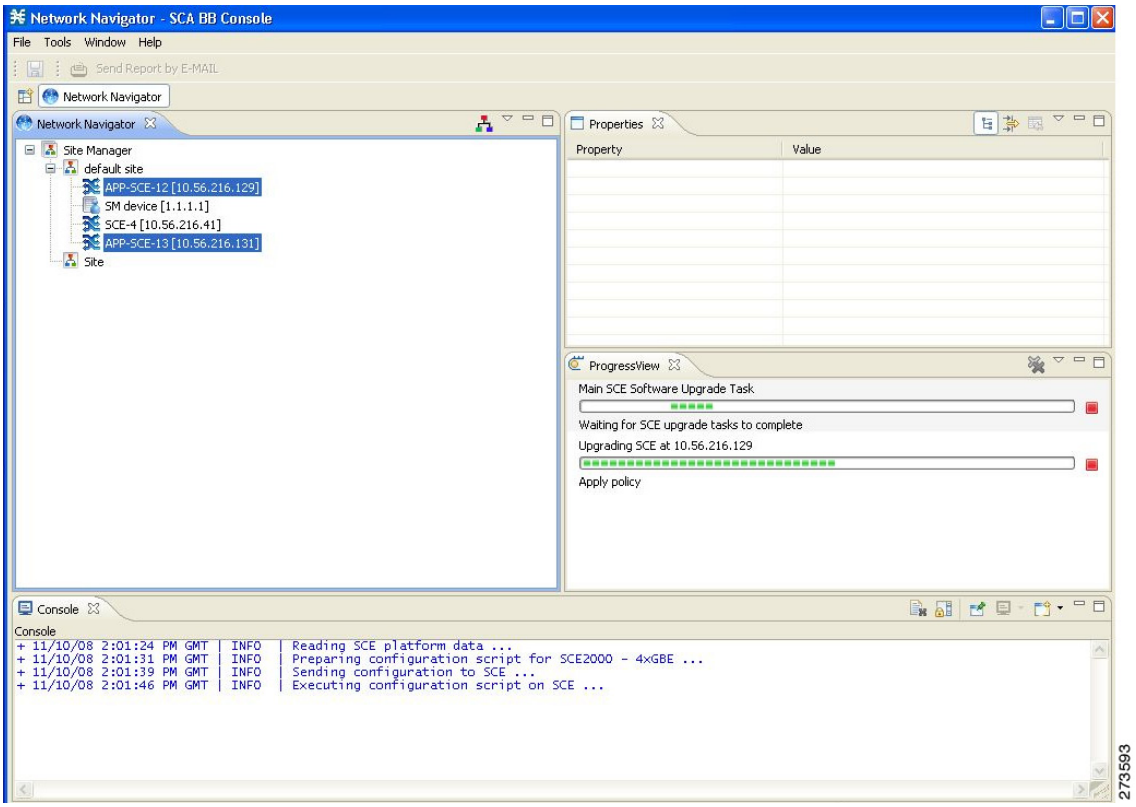
Click **Run in Background** to run the upgrade in the background.

Figure 12 Main SCE Software Upgrade Task Window



The upgrade runs in the background (see Figure 13).

Figure 13 Network Navigator



Upgrading Cascaded SCE Platforms

In a high availability deployment, a pair (or pairs) of SCE platforms are cabled in a cascaded setup, providing SCE platform redundancy. This type of a deployment requires the following steps when upgrading.

Step 1 Select the standby SCE platform or platforms in the SCE Software Upgrade Wizard.

Step 2 When the upgrade is complete, force failure in all the active SCE platforms:

```
SCE> enable 10
<password>
SCE# config
SCE(config)#interface linecard 0
SCE(config if)# force failure-condition
```

This makes the updated SCE platforms the active ones, and they begin to give the new service.

Step 3 Run the SCE Software Upgrade Wizard again, this time selecting the remaining SCE platforms, which were originally the active platforms and now are the standby SCE platforms.

Make sure to specify the same upgrade files that you used in Step 1.

Because this includes a reboot, it is not necessary to undo the **force failure** command.

6 Upgrade Procedure Limitations

SCE Platform

Link Downtime Due to LIC Re-Burning

Link downtime is expected during SCE platform upgrade (the LIC chip firmware is reburned). The expected downtime depends on the system's auto-negotiation configuration, and can be up to one minute.

Misclassification of Flows Initiated Prior to Upgrade Completion

Flows that were initiated before upgrade completion can be misclassified. Gradual classification restoration is expected when SCE software upgrade is completed, or when a standby SCE becomes active. This reclassification is needed because the flow's previous classification decision is lost. This reclassification would usually be inaccurate because an accurate classification depends on analyzing the beginning of the flow. Therefore, the flow would usually be reclassified according to the corresponding Generic or Behavioral signature. This downtime ends when all these reclassified flows are closed.

Service Downtime

Service downtime is expected during SCE platform upgrade on non-High Availability setups and on High Availability setups.

- On non-High Availability setups, the SCE platform does not perform traffic classification, reporting, and control during the SCE platform upgrade. These capabilities are restored after upgrade completion (restoration is gradual, due to misclassification of traffic flows that were initiated prior to upgrade completion). See "Misclassification of Flows Initiated Prior to Upgrade Completion" section on page 29 for further information.
- On High Availability setups, service downtime is not expected (as the cascaded SCE platforms alternate on upgrade), except for gradual service buildup when switching SCE platforms due to misclassification of traffic flows that were initiated prior to upgrade completion. See "Misclassification of Flows Initiated Prior to Upgrade Completion" section on page 29 for further information.

Loss of Aggregated Unreported Data

During SCE platform upgrade, subscriber quota and usage information maintained in the SCE platform that was not reported to a collection system is lost. Depending on the system data export frequency (configurable through periods between RDRs of all sorts), the amount of such information can be kept to a minimum.

This is true also for High Availability configurations.

Loss of Configuration

Any non-default assignments of RDR tags to categories are lost when upgrading; the default mapping is restored after the upgrade. If any non-default assignments were made, you should reconfigure them manually after the upgrade.

SCA BB Clients and Service Configuration

SCA BB Console, which incorporates the service configuration editor, SM GUI, and Reporter, is not backward compatible and can work only with the 3.6.5 system components (SCE platform, CM, SM).

SCA BB Console Interoperability

Version 3.6.5 of the Network Navigator cannot apply service configurations to previous versions of the SCE platforms. Nevertheless, the Network Navigator 3.6.5 can upgrade the SCE platform to 3.6.5, and then service configurations can be applied.

Reporter and DB Interoperability

The Reporter and Reporter Templates of 3.6.5 can be used to create reports from an earlier-version database, provided that the same reports existed in the earlier version. However, reports that are new in 3.6.5 cannot be created when connecting to an earlier-version database.

Running Two SCA BB Consoles or Reporters

Running two SCA BB Consoles or Reporters of different versions on the same machine is not supported and should be avoided.

Subscriber Manager

In non-High Availability Subscriber Manager setups, the SM upgrade procedure causes downtime for subscriber provisioning and subscriber status awareness (LEG communication).

Quota Manager

If the QM is not deployed as a cluster, service downtime is expected. This is the same service downtime that is expected during an SM upgrade.

Collection Manager

Upgrading the CM imposes downtime for the upgraded machine during the entire process. To avoid data collection downtime, an alternate CM can be used (for either bundled or unbundled configurations).

Sending RDRs to an alternate CM is supported by the SCE platform.

Configuration

When upgrading the CM to 3.6.5, the users configuration on the CM server (the PRPC users file, prpc.usr) is deleted. It is necessary to redefine the users after the upgrade is completed.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

Printed in the USA on recycled paper containing 10% postconsumer waste.

OL-21070-03

7 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.