Cisco Service Control Solution Guide

Cisco Service Control Guide to Upgrading to Cisco SCA BB 3.7.x

Revised: August 22, 2012, OL-24176-03

Note This document supports all 3.7.x releases.

1 Overview

Upgrading from Version 3.5.x, or 3.6.x to Version 3.7.x

This guide describes the process of upgrading the Cisco Service Control solution from Version 3.5.x, or 3.6.x to Version 3.7.x. It describes the upgrade process for each of the four components:

- Cisco 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 3.5.x or SCA BB 3.6.x operating concurrently (using the same Collection Manager and Subscriber Manager 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 Cisco SCA BB.

a. Install the 3.7.x console.

b. (Optional) Install the Cisco SCA BB Service Configuration Utility Version 3.7.x, **servconf,** in an empty directory.

Step 2 Upgrade the Subscriber Manager (or Subscriber Manager cluster) according to the procedure described in Chapter 3, "Upgrading the Subscriber Manager".

a. Run the Subscriber Manager upgrade script.

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

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

Step 3 Deploy a new Collection Manager running 3.7.x. See Chapter 4, "Upgrading the Collection Manager".

- If additional Collection Manager and database are deployed for the transition phase (two Collection Manager databases in total, regardless of whether the configuration is bundled), collection works for all SCE platforms (both older versions and 3.7.x). For nonbundled databases, there may be several ways to implement this; consult a database specialist if you are using a nonbundled database.
- Each Collection Manager collects Raw Data Records (RDRs) from a single version to a distinct database (either bundled or nonbundled) and comma-separated values (CSV) repository.

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

- Make sure the upgraded SCE platform RDRs are directed to the Collection Manager that runs version 3.7.x. Service downtime (from a collection perspective) depends on the Collection Manager configuration that you have implemented (single or dual) during the upgrade.

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

Step 5 (If two Collection Manager are used during the upgrade) Remove the Collection Manager running the former version after upgrading all the SCE platforms.

Supported Working Configurations

The Cisco SCA BB release 3.7.x supports a combination of component versions:

- Cisco Service Control Operating System (SCOS) 3.7.x
- Application - SCA BB 3.7.x (PQI for installation on SCE platform)
- SCMS Subscriber Manager 3.7.x (if a Subscriber Manager is required for the deployment)
- SCMS Collection Manager 3.7.x (if a Collection Manager is required for the deployment)

Note This document covers the upgrade of a system that includes a Subscriber Manager and a Collection Manager. 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. You require the new PQI file to run this command. However, the **PQI uninstall file** command works only if the PQI was installed from the CLI, and not from the SCA BB Console. But, installing the older package will overwrite the PQI.

2 Upgrading the Cisco SCA BB

This chapter details the procedure for upgrading from a functional Cisco SCA BB 3.5.x, or Cisco SCA BB 3.6.x deployment to Cisco SCA BB 3.7.x.

Upgrading Cisco SCA BB

Upgrading Cisco SCA BB consists of two steps:

1. Installing the 3.7.x console. (It is not necessary to uninstall the previous version.)
2. (Optional) Installing the 3.7.x service configuration utility.

How to Install the Console

Navigate to the console installation file, sca-bb-console-3.7.x.exe, and double-click it.

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

How to Upgrade the Cisco SCA BB Service Configuration Utility

To upgrade the Cisco SCA BB service configuration utility, complete these steps:

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

Step 2 Unpack the file to a new folder.

The following files are under the bin folder:

- The SCA BB Service Configuration Utility (servconf)
- The SCA BB Real-Time Monitoring Configuration Utility (rtmcmd) and associated real-time monitoring report templates
- The SCA BB Signature Configuration Utility (sigconf)

3 Upgrading the Subscriber Manager

This chapter describes how to upgrade the Cisco Service Control Management Suite Subscriber Manager.

Contents of the Distribution Files

The SCMS Subscriber Manager components are supplied in three distribution files:

- Subscriber Manager for Solaris
- Subscriber Manager for Linux 32
- Subscriber Manager for Linux 64
- 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 *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 Subscriber Manager version that was previously installed and the requirement (or lack of requirement) for fail-over in the new installation.

The following sections provide details on three types of upgrade procedures:

- How to Upgrade a Standalone Setup, page 7
- How to Upgrade from 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 you 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 Subscriber Manager for the upgrade, configure the system kernel configuration file on the Subscriber Manager.

Subscriber Manager database requires that certain changes be made in the operating system kernel configuration file:

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

These changes increase the shared memory and semaphore resources on Solaris machines from their defaults.

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 required 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 Subscriber Manager. The sizing requirements of your system affect only the shared memory size. To determine the correct configuration values for your system, “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 SMdatabase
  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 SMdatabase
  ```

Note For Solaris, mention the shared memory settings as hexadecimal value in /etc/system file.

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

How to Upgrade a Standalone Setup

Note To upgrade from Version 3.5.5 to Version 3.7.x, you must first upgrade to Version 3.6.0 and then to 3.7.x. To upgrade from Version 2.x to Version 3.6, you must first upgrade to Version 3.0 or 3.1. You can upgrade directly from Version 3.6.5 to Version 3.7.x.

The following upgrade procedure is supported only by Release 3.x software versions. To upgrade the Subscriber Manager from a Release 2.x software version, you must first upgrade the Subscriber Manager environment to a Release 3.1.x software version and then perform an additional upgrade to Release 3.6.0.

For more information about how to upgrade from a Release 2.x software version to a Release 3.1.x software version, refer to the Release 3.1.x manuals.

This procedure applies to the Subscriber Manager 3.0.x and later.

This upgrade procedure requires service down-time.

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

Step 1 Extract the distribution files.

Before you upgrade the Subscriber Manager, 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 Subscriber Manager.

c. Unzip the files by 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 "Configuring the Required Memory Settings" section on page 6. For further information, see the *Cisco Service Control Product Installation Guide*.

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

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

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

Note For Linux—64-bit or 32-bit JVM and database.

Note If the **/etc/motd** file exists, you can not run the script. Move or remove the file before you run 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.

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 from a Standalone Setup to a Cluster Setup

Note To upgrade from Version 3.5.5 to Version 3.7.x, you must first upgrade to Version 3.6.0 and then to 3.7.x. You can upgrade directly from Version 3.6.5 to Version 3.7.x.

The following upgrade procedure is supported only from Release 3.x software versions. To upgrade Subscriber Manager from a Release 2.x software version, you must first upgrade the Subscriber Manager environment to a Release 3.1.x software version and then perform an additional upgrade to Release 3.6.0. From Version 3.6.0, you can upgrade to Version 3.7.x.

For more information about how to upgrade from Release 2.x software to Release 3.1.x software, the Release 3.1.x manuals. For details on how to upgrade to Version 3.6.0, see the Subscriber Manager 3.6.x manuals.

This section describes the procedure for upgrading from a standalone setup to a cluster setup. This procedure applies to the Subscriber Manager from version 3.0.x and later.

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 Subscriber Manager 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 Subscriber Manager machine and SM-B is the new Subscriber Manager 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 the "How to Upgrade a Standalone Setup" section on page 7.

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

Step 4 Replicate the Subscriber Manager 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 by 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.

>p3db --set-rep-scheme

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

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 by using the following CLU command:

p3sm --load-config

b. Make SM-B standby.

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

c. Ensure that SM-A is active.

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

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

- You can upgrade directly from Cisco SCMS Subscriber Manager (SM) Version 3.6.5 to SM Version 3.7.x. However, to upgrade from SM Version 3.5.5 or earlier to SM Version 3.7.x, you must first upgrade to SM Version 3.6.0 and then to SM Version 3.7.x. To upgrade from SM Version 2.x to SM Version 3.6, you must first upgrade to SM Version 3.0 or SM Version 3.1.
- 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 3.7.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 10.
- Understand the scripts used while upgrading a cluster setup. For details, see the "Understanding the Scripts Used During Upgrade" section on page 10.

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 10.
- install-vcs-agents.sh. For details, see the "Understanding the install-vcs-agents.sh script" section on page 11.

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 10.
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 No.	Action	Notes
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 10
Step 7	Wait until the cluster-upgrade.sh script finishes all tasks.	—
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 Veritas Cluster Server (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 No.	Action	Notes
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 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 No.	Action	Notes

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 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 Subscriber Manager to an earlier 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 Subscriber Manager downgrade.

4 Upgrading the Collection Manager

This chapter describes the procedures for upgrading the Collection Manager.

When upgrading a complete system, it is recommended that you install a second Collection Manager running the new version and then uninstall the Collection Manager running the earlier version. This procedure provides a seamless transition to the new version. In this case, no upgrade procedure is run on the Collection Manager.

Note You can upgrade to Collection Manager Version 3.7.x only from Collection Manager Version 3.6.x.

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

How to Upgrade the Collection Manager to Version 3.7.x

Step 1 Get the Collection Manager software as described in the *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 The Collection Manager 3.7.x version also works with the Cisco Service Control solution in combination with the Cisco ASR 1000 Series Aggregation Services Routers and Cisco IOS NetFlow. You will be prompted to enable the NetFlow support during the upgrade. Ignore this option, if you are upgrading only SCE RDR collection process.

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 for five minutes before you run this script.

5 Upgrading the SCE Platform Software

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

Note You can upgrade SCE Platform Software from Version 3.5.x or 3.6.x to 3.7.x.

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 that you do the following:

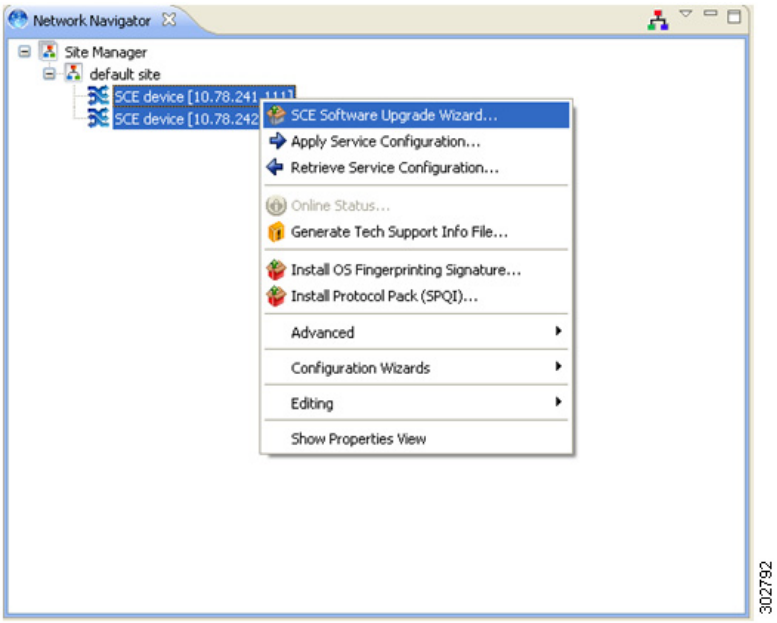
- (If the IP address of all SCE platforms to be upgraded are not defined in the Network Navigator) Gather the IP addresses of all SCE platforms to be upgraded.
- Download the relevant pkg file, pqi file, and protocol pack to a local location or to a location accessible by FTP. If using an FTP site, make 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 reapplies after the upgrade is complete.
  - *Service Configuration from a Local File*—Specifies the pqb file to be applied.

How to Upgrade the Cisco SCE Platform Software

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

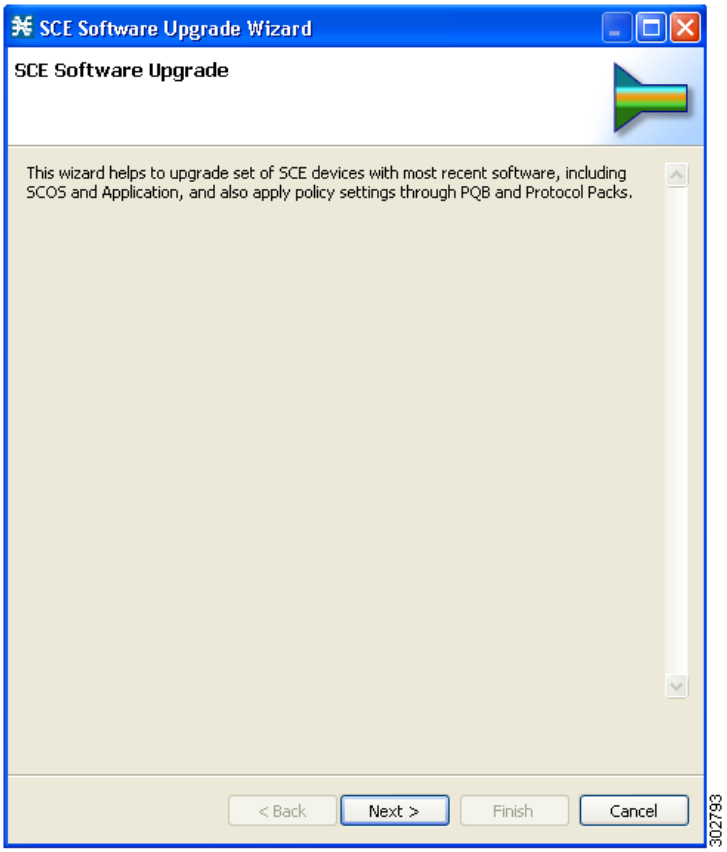
If the Cisco SCE platforms are not yet defined in the Network Navigator, you can select the site node.

Figure 1 Network Navigator



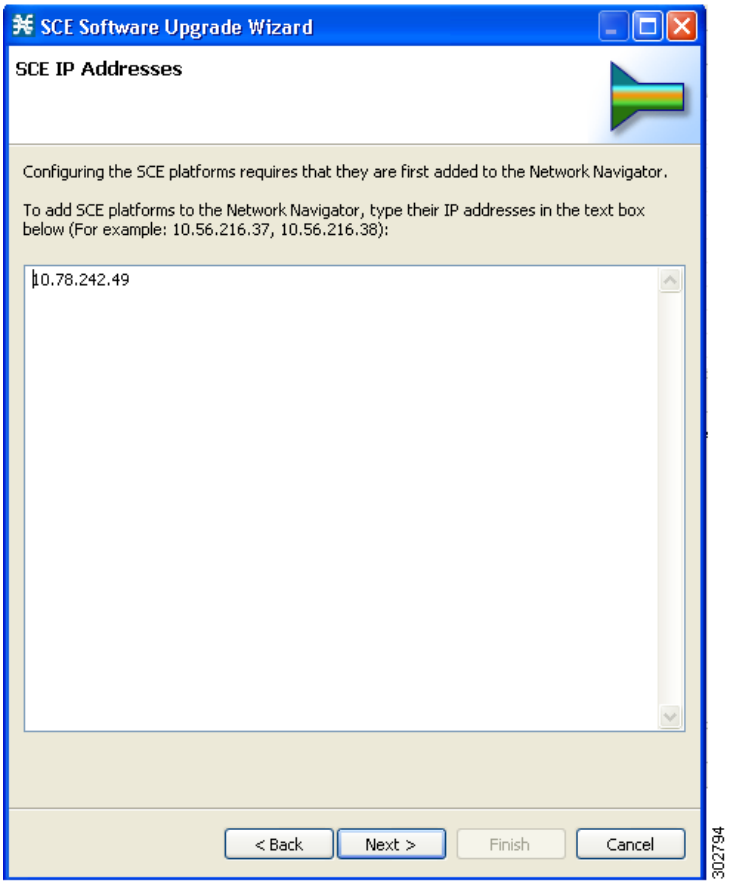
The SCE Software Upgrade Wizard opens. Click **Next**(see Figure 2).

Figure 2 SCE Software Upgrade Wizard



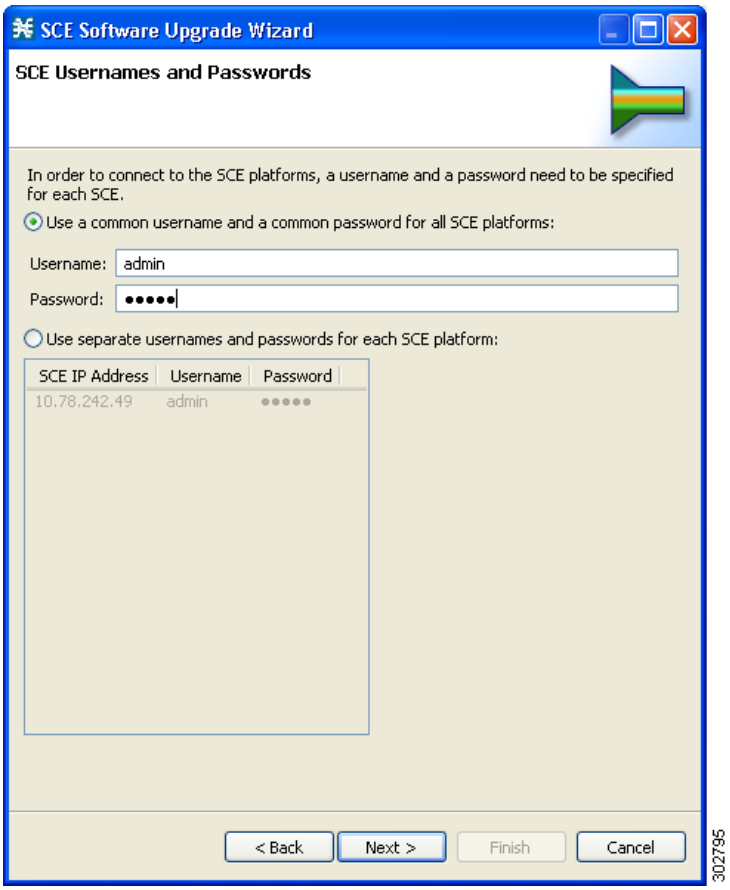
Step 2 In the SCE IP Addresses pane (see Figure 3), verify that the IP addresses of all the Cisco SCE platforms to be upgraded are displayed. If any of the IP addresses are not displayed, enter the details and click **Next**.

Figure 3 SCE Software Upgrade Wizard—SCE IP Addresses



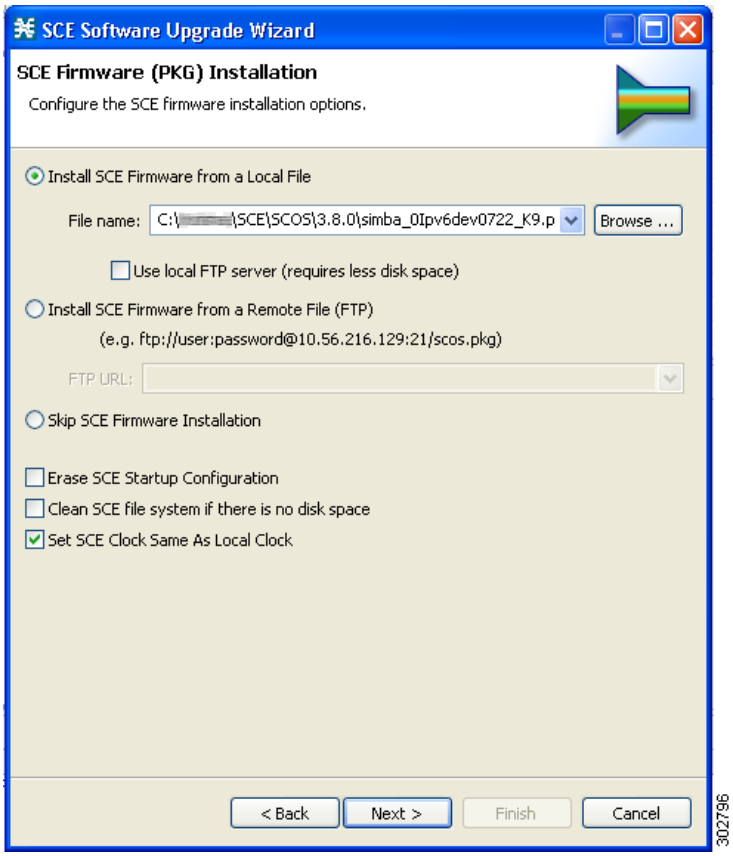
Step 3 In the SCE Usernames and Passwords pane (see Figure 4), enter the username and password required to access the Cisco SCE platform. You can use the same username and password for all the platforms or enter a different username and password for each platform and click **Next**.

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



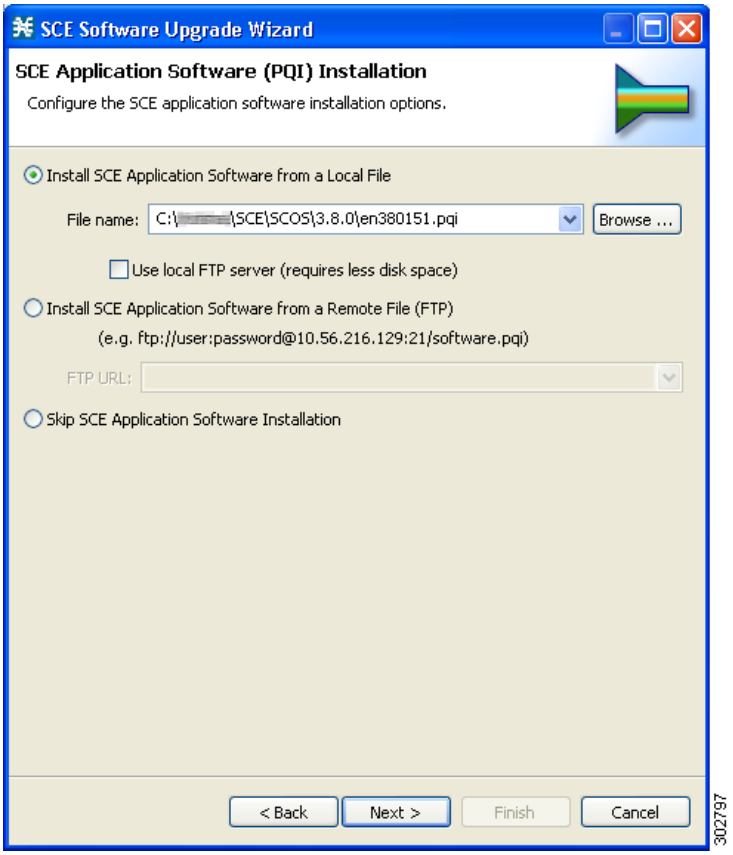
Step 4 In the SCE Firmware (PKG) Installation pane (see Figure 5), specify the location of the firmware file to be installed on all the selected Cisco SCE platforms and click **Next**.

Figure 5 SCE Software Upgrade Wizard—SCE Firmware (PKG) Installation



Step 5 In the SCE Application Software (PQI) Installation pane (see Figure 6), specify the location of the PQI file to be installed on all the selected Cisco SCE platforms and click **Next**.

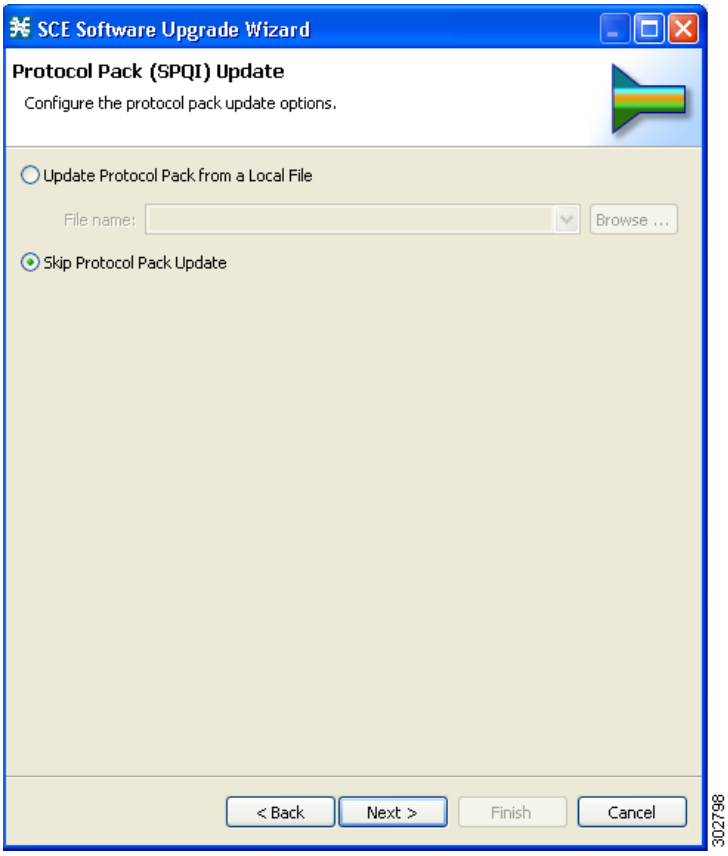
Figure 6 SCE Software Upgrade Wizard—SCE Application Software (PQI) Installation



Step 6 In the Protocol Pack (SPQI) Update pane (see Figure 7), check Skip Protocol Pack Update and click **Next**.

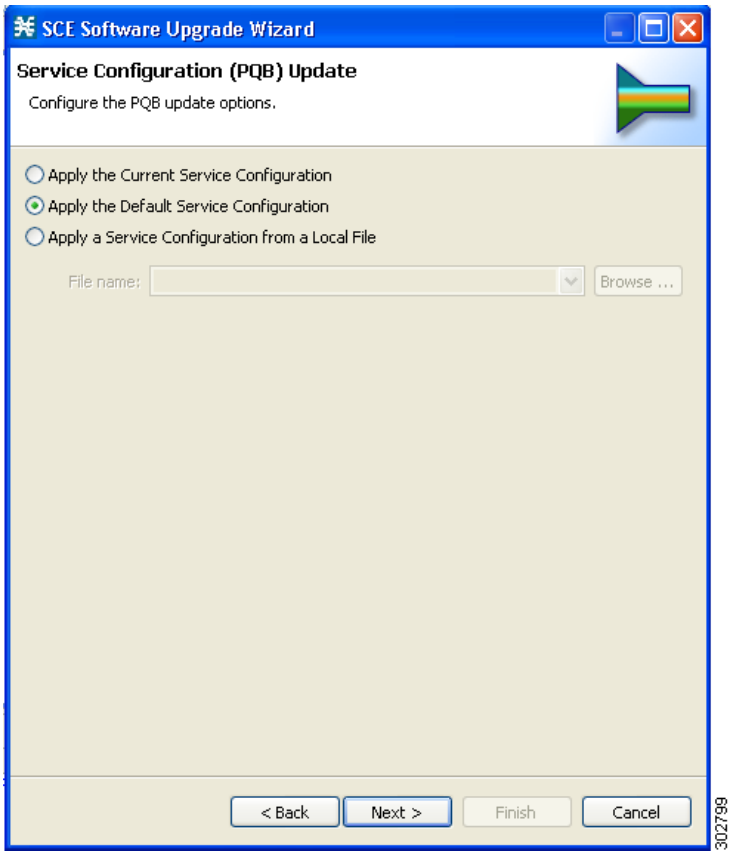
Note If you install the protocol pack during the upgrade, it must be the same version or a later version of the protocol pack you are upgrading from.

Figure 7 SCE Software Upgrade Wizard—Protocol Pack (SPQI) Update



Step 7 In the Service Configuration (PQB) Update pane (see Figure 8), check Apply the Default Service Configuration and click **Next**.

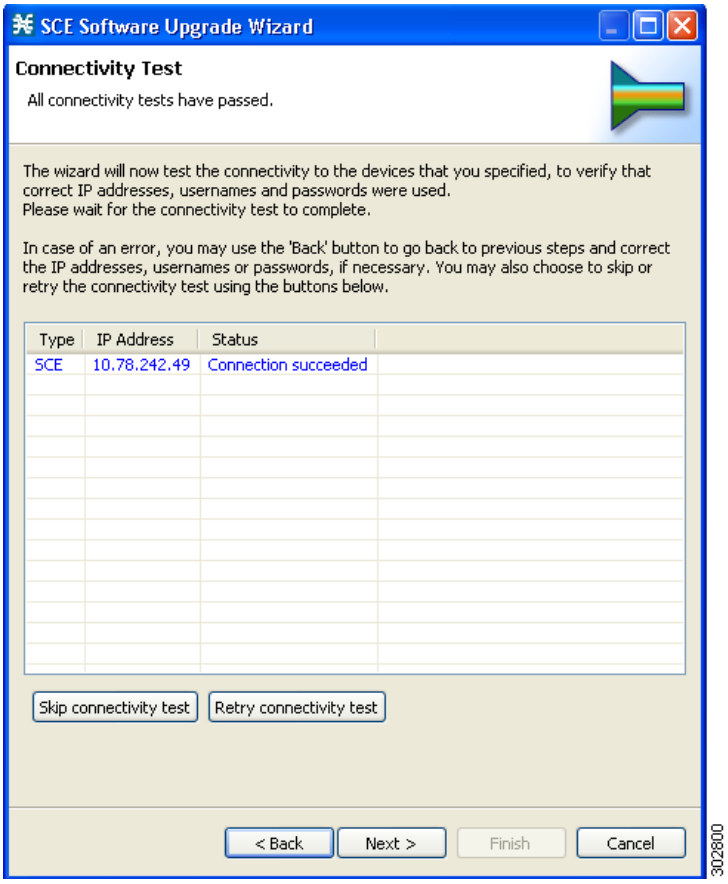
Figure 8 SCE Software Upgrade Wizard—Service Configuration (PQB) Update



Step 8 The Connectivity Test pane of the SCE Software Upgrade Wizard is displayed (see Figure 9). Click **Next**.

Note If a connection to one or more devices cannot be made, or if there is a 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**.

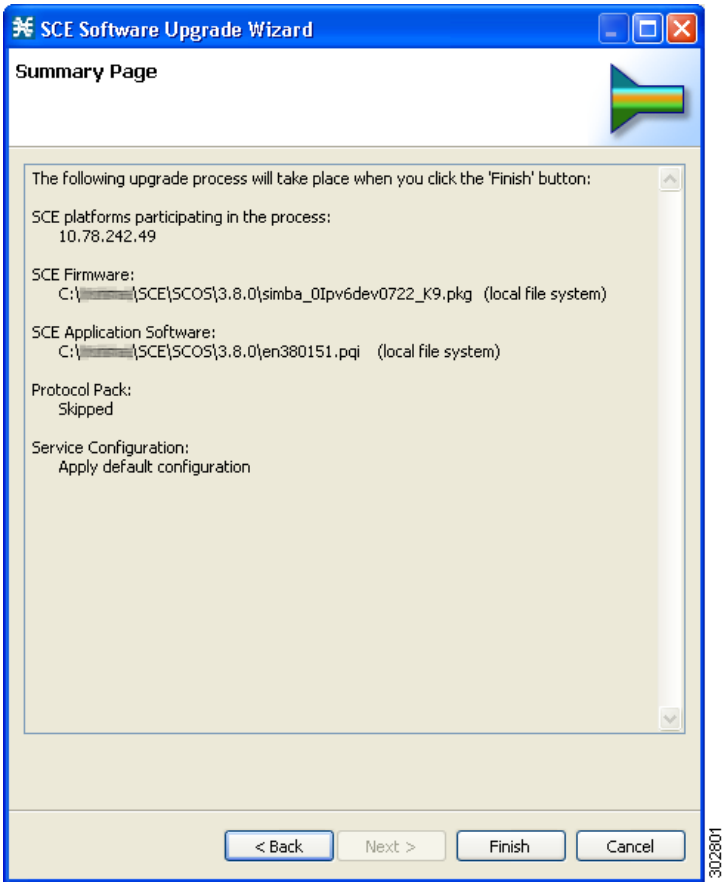
Figure 9 Connectivity Test



Step 9 The Summary pane summarizes all the information (see Figure 10). Verify that all the IP addresses and file locations are correct. In this pane, you can:

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

Figure 10 SCE Software Upgrade Wizard—Summary



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 is 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 installed PKG file is retrieved.

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):

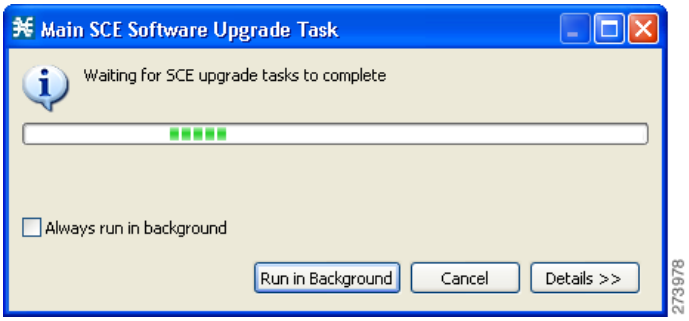
- Retrieve the current service configuration from the SCE platform (only if the current service configuration is going to be reinstalled after the upgrade).
- Uninstall the existing application software (PQI).
- Upgrade SCE platform firmware (PKG).
- Install application software (PQI).
- Apply service 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 10 The system keeps you informed of the progress of the upgrade (see Figure 11).

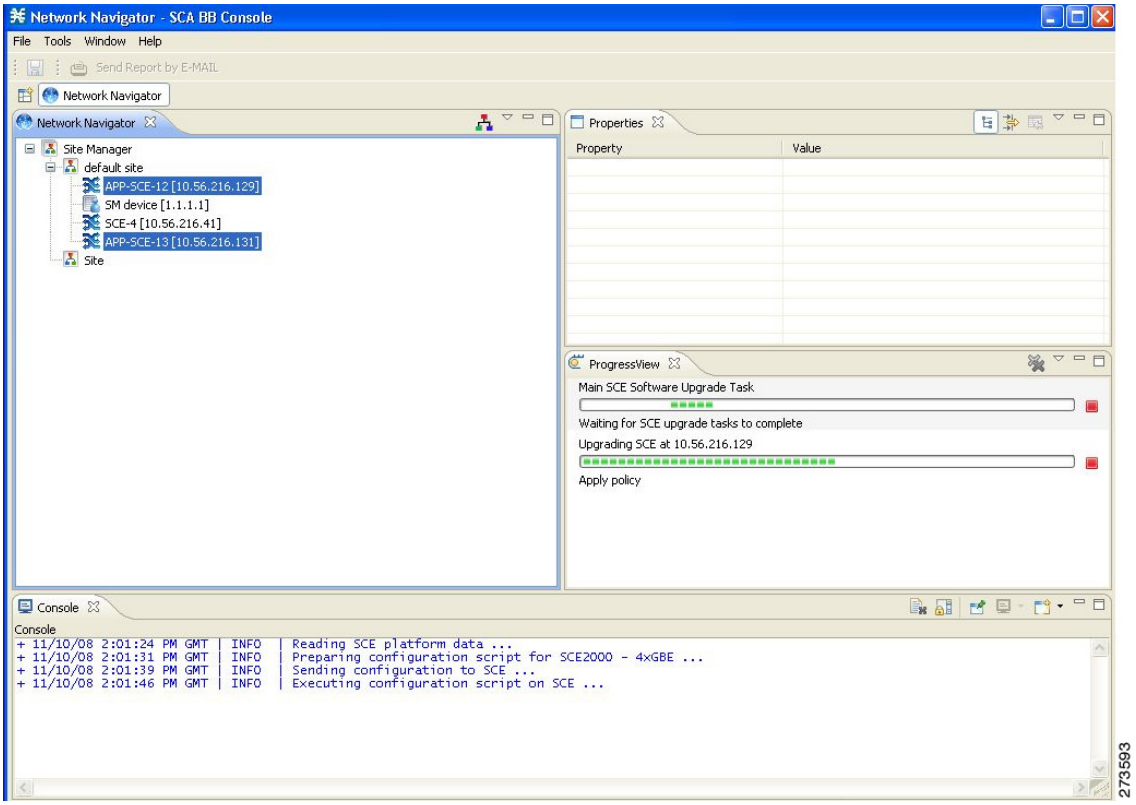
Click **Run in Background** to run the upgrade in the background.

Figure 11 Main SCE Software Upgrade Task



The upgrade runs in the background (see Figure 12).

Figure 12 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 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 step makes the upgraded SCE platforms the active ones, and they begin to give the new service.

Step 3 Run the SCE Software Upgrade Wizard on the remaining SCE platforms; platforms that were originally the active platforms and now are the standby platforms.

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

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

6 Upgrade Procedure Limitations

This chapter provides details of limitations to the Cisco Service Control solution upgrade procedure.

SCE Platform

Link Downtime Because of LIC Re-Burning

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

Misclassification of Flows Initiated Before 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 previous classification decision of the flow 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 before upgrade completion). See the "Misclassification of Flows Initiated Before Upgrade Completion" section on page 31 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 because of misclassification of traffic flows that were initiated before upgrade completion. See the "Misclassification of Flows Initiated Before Upgrade Completion" section on page 31 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, Subscriber Manager GUI, and Reporter, is not backward compatible and can work only with the 3.7.x system components (SCE platform, Collection Manager, and Subscriber Manager).

Cisco SCA BB Console Interoperability

Version 3.7.x of the Network Navigator cannot apply service configurations to earlier versions of the SCE platforms. Nevertheless, the Network Navigator 3.7.x can upgrade the SCE platform to 3.7.x, and then service configurations can be applied.

Reporter and Database Interoperability

The Reporter and Reporter Templates of 3.7.x can be used to create reports from an earlier-version database, only if the same reports existed in the earlier version. However, reports that are new in 3.7.x cannot be created when connecting to an earlier-version database.

Running Two Cisco SCA BB Consoles or SCA Reporters

Running two SCA BB Consoles or SCA 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 Quota Manager is not deployed as a cluster, service downtime is expected. This downtime is the same service downtime that is expected during a Subscriber Manager upgrade.

Collection Manager

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

The SCE platform supports sending RDRs to an alternate Collection Manager.

Configuration

When upgrading the Collection Manager to Version 3.7.x, the user configuration on the Collection Manager 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-24176-03

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.