



CISCO SERVICE CONTROL SOLUTION GUIDE



Cisco Service Control Guide to Upgrading to Cisco SCA BB 5.0.x

- 1** [Overview](#)
- 2** [Upgrading the Cisco SCA BB](#)
- 3** [Upgrading the Subscriber Manager](#)
- 4** [Upgrading the Cisco Service Control Collection Manager](#)
- 5** [Upgrading the SCE Platform Software](#)
- 6** [Upgrade Procedure Limitations](#)
- 7** [Obtaining Documentation and Submitting a Service Request](#)

1 Overview

Upgrading from Version 4.0.x or 4.1.x to Version 5.0.x

This guide describes the process of upgrading the Cisco Service Control solution from Version 4.0.x or 4.1.x to Version 5.0.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.x, 4.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 5.0.x console.
- b. (Optional) Install the Cisco SCA BB Service Configuration Utility Version 5.0.x, **servconf**, in an empty directory.

Step 2 Upgrading the Subscriber Manager from older version to the Subscriber Manager 5.0.x is not supported. However, you can migrate from Version 4.1.x configuration to Version 5.0.x configuration using the **upgrade-cfg.sh** script.

Step 3 Deploy a new Collection Manager running 5.0.x. See Chapter 4, “[Upgrading the Cisco Service Control Collection Manager](#)”.

- If additional Collection Manager and database are deployed for the transition phase (two Collection Manager databases in total, collection works for all SCE platforms (both older versions and 5.0.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 and comma-separated values (CSV) repository.

Step 4 You need to replace Cisco SCE 8000 device with Cisco SCE 10000 device and upgrade the SCE platform software by using the SCE Software Upgrade Wizard. For more information on Cisco SCE 10000 device installation, see [Cisco SCE 10000 Installation and Configuration Guide](#).

- Make sure the upgraded SCE platform RDRs are directed to the Collection Manager that runs version 5.0.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 5.0.x supports a combination of component versions:

- Cisco Service Control Operating System (SCOS) 5.0.x
- Application - SCA BB 5.0.x (PQI for installation on SCE platform)
- Cisco Service Control Subscriber Manager 5.0.x (if a Subscriber Manager is required for the deployment)
- Cisco Service Control Collection Manager 5.0.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 for Cisco SCE 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. If SCA BB PQI or SPQI is installed from SCA BB Console, use the **no application** command to remove the application.



Note Cisco SCE does not support direct downgrade of higher PP versions to a lower PP version. While downgrading the protocol pack from a higher version to a lower version, the Cisco SCA BB console displays an error message and prevents you from applying the policy on the Cisco SCE.

2 Upgrading the Cisco SCA BB

This chapter details the procedure for upgrading from a functional Cisco SCA BB 4.0.x or 4.1.x deployment to Cisco SCA BB 5.0.x.

Upgrading Cisco SCA BB

Upgrading Cisco SCA BB consists of two steps:

1. Installing the 5.0.x console.
2. (Optional) Installing the 5.0.x service configuration utility.

How to Install the Console

Navigate to the console installation file, `sca-bb-console-5.0.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 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 Signature Configuration Utility (`sigconf`)
-

3 Upgrading the Subscriber Manager



Note

Upgrading the Subscriber Manager from older version to the Subscriber Manager 5.0.x is not supported. However, you can migrate from Version 4.1.x configuration to Version 5.0.x configuration using the `upgrade-cfg.sh` script.

Contents of the Distribution Files

The Cisco Service Control Subscriber Manager components are supplied in three distribution files:

- 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 6](#)
- [How to Upgrade from a Standalone Setup to a Cluster Setup, page 7](#)
- [How to Upgrade a Cluster Setup, page 8](#)

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.

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 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 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

Upgrading the Subscriber Manager from older version to the Subscriber Manager 5.0.x is not supported. However, you can migrate from Version 4.1.x configuration to Version 5.0.x configuration using the `upgrade-cfg.sh` script.

The following upgrade procedure is supported only by Release 3.x software versions. You can directly upgrade from version 3.7.2 or 3.8.x to 4.0.0. 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. To upgrade from Version 3.5.5 to Version 3.7.0, you must first upgrade to Version 3.6.0 and then to 3.7.0. You can upgrade directly from Version 3.6.5 to Version 3.7.0. To upgrade from Version 3.7.0 to Version 3.8.5, you must first upgrade to Version 3.8.0 and then to 3.8.5.

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 4.1.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 7.

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 5. 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 Linux—64-bit VM 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

Upgrading the Subscriber Manager from older version to the Subscriber Manager 5.0.x is not supported. However, you can migrate from Version 4.1.x configuration to Version 5.0.x configuration using the upgrade-cfg.sh script.



Note

You can directly upgrade from Version 3.8.x or 4.0.x to Version 4.1.x. You can upgrade directly from version Version 3.7.x or 3.8.x to version 4.0.x. To upgrade from Version 3.5.5 to Version 3.7.0, you must first upgrade to Version 3.6.0 and then to 3.7.0. You can upgrade directly from Version 3.6.5 to Version 3.7.0. To upgrade from Version 3.7.0 to Version 3.8.5, you must first upgrade to Version 3.8.0 and then to 3.8.5.

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 3.7.0.

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. For details on how to upgrade to Version 3.7.0, see the Subscriber Manager 3.7.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 6.



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, page 8](#)
- [Upgrading a Cluster Setup, page 10](#)

Before You Start



Note Upgrading the Subscriber Manager from older version to the Subscriber Manager 5.0.x is not supported. However, you can migrate from Version 4.1.x configuration to Version 5.0.x configuration using the `upgrade-cfg.sh` script.

- You can upgrade from Version 3.8.x or 4.0.x to Version 4.1.x. You can upgrade from Version 3.8.x to Version 4.0.x. You can also upgrade directly from Cisco Service Control Subscriber Manager (SM) Version 3.6.5 to SM Version 3.7.0 or Version 3.7.x to Version 3.8.x. However, to upgrade from SM Version 3.5.5 or earlier to SM Version 3.7.0, you must first upgrade to SM Version 3.6.0 and then to SM Version 3.7.0. 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 Service Control Subscriber Manager on your operating system:
 - 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 Service Control Subscriber Manager to a cluster setup with the latest version of the Cisco Service Control 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



Note

Upgrading the Subscriber Manager from older version to the Subscriber Manager 5.0.x is not supported. However, you can migrate from Version 4.1.x configuration to Version 5.0.x configuration using the upgrade-cfg.sh script.

To upgrade a cluster setup, complete the following steps:

Step No.	Action	Notes
Step 1	<p>Configure the system kernel configuration file on both the machines:</p> <ol style="list-style-type: none"> Configure the system kernel configuration file on the standby Subscriber Manager. Reboot the standby SM. 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. Run the following VCS CLU command from /opt/VRTSvcs/bin: <pre>#./hagrp -switch service group name -to System</pre> Repeat Step a. and Step b. on the new standby Subscriber Manager. 	<p>Before starting the upgrade procedure, configure the system kernel configuration file on both the machines.</p> <p>For details about the system kernel configuration procedure, see the “Configuring the Required Memory Settings” section on page 5.</p>
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	<p>Stop VCS monitoring on the standby machine:</p> <ol style="list-style-type: none"> Log in as the <i>root</i> user. Use the following VCS CLU command from /opt/VRTSvcs/bin to stop VCS monitoring of the Subscriber Manager: <pre>#./hastop -local</pre> 	—
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 5.	For details about the required memory settings, see the <i>Cisco Service Control Product Installation Guide</i> .

Step No.	Action	Notes
Step 5	<p>Pause database replication on the active machine:</p> <ol style="list-style-type: none"> On the active machine, change the directory to the location where you extracted the distribution files. Run this CLU command from the scripts directory: <code>p3db --rep-pause</code> Run this CLU command from the scripts directory and verify that replication is in <i>pause</i> state: <code>p3db --rep-status</code> Return to the standby machine. 	This step is applicable only when upgrading the first Subscriber Manager machine.
Step 6	<p>Run the cluster-upgrade.sh script on the standby machine: <code># cluster-upgrade.sh [command-options]</code></p> <p>Do not start the SM after running cluster-upgrade.sh.</p>	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 8	<p>Stop the replication and start the SM on the standby machine.</p> <p>The following steps should be performed <i>only when performing upgrade on the first machine</i>.</p> <ol style="list-style-type: none"> Stop the SM replication: <code>-bash-3.1\$ p3db --rep-stop</code> Start the SM: <code>-bash-3.1\$ p3sm --start --wait</code> Use the <code>p3sm</code> CLU command to verify the status of the SM. <code>-bash-3.1\$ p3sm --sm-status</code> 	<p>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.</p> <p>The SM boot time after the upgrade will be longer than usual due to the extra time taken to initialize the database indexes.</p> <p>If the SMS-STATUS indicates a failure, <i>stop the upgrade</i>. For details on troubleshooting the SM in failure mode, see the <i>Cisco Service Control Management Suite Subscriber Manager User Guide</i>.</p>
Step 9	<p>Run the install-vcs-agents.sh script on the standby machine: <code># install-vcs-agents.sh [command-options]</code></p>	—
Step 10	<p>Restart Veritas Cluster Server (VCS) monitoring on the standby machine:</p> <ol style="list-style-type: none"> Run the following VCS CLU command from <code>/opt/VRTSvcs/bin</code>: <code>#./hastart</code> VCS monitoring starts the SM process automatically in the initialization state. Use the <code>p3sm</code> CLU command to check whether the SM is up: <code>-bash-3.1\$ p3sm --sm-status</code> Use the <code>p3cluster</code> CLU command to set the SM to the standby state: <code>-bash-3.1\$ p3cluster --standby</code> 	<p>The <code>./hastart</code> command starts the replication agent that updates the database schema on the active machine.</p> <p>After this operation is performed, you cannot downgrade to an earlier version.</p>

Step No.	Action	Notes
Step 11	<p>Continue database replication on the active machine:</p> <ol style="list-style-type: none"> On the <i>Active</i> machine, change the directory to the location where you extracted the distribution files. Run the <code>--rep-continue</code> CLU command. Run the <code>--rep-status</code> CLU command and verify that replication is in the <i>start</i> state. Return to the standby workstation. 	This step is applicable only when upgrading the first machine and only if Step 5 was performed.
Step 12	<p>Verify that the changed data has been replicated.</p> <p>Wait until the replication of all the data that was changed while the upgrade script was running.</p> <ul style="list-style-type: none"> On the active Subscriber Manager add a dummy subscriber using the <code>p3subs</code> CLU: <pre>-bash-3.1\$ p3subs --add -s dummySub</pre> On the standby Subscriber Manager, login as <i>root</i> user, and run the <code>p3subs show</code> command: <pre># p3subs --show -s dummySub</pre> 	When upgrading the second Subscriber Manager, add a subscriber with a name other than <i>dummySub</i> 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 Service Control SM LEGs User Guide .
Step 14	<p>Manually trigger a failover using the Veritas Cluster Manager and wait until the standby SM becomes active and the active SM becomes the standby:</p> <p>Run the following VCS CLU command from <code>/opt/VRTSvcs/bin</code>:</p> <pre># hagrps -switch service group name -to System</pre>	<p>For more information about the <code>hagrps</code> CLU command, refer to your Veritas Cluster Server documentation.</p> <p>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.</p>
Step 15	<p>Repeat the upgrade procedure on the standby SM.</p> <p>To upgrade the second SM, repeat the procedure from Step 2. But, do not perform Step 5, Step 8, and Step 11.</p>	—

Step No.	Action	Notes
Step 16	<p>Upgrade the database replication protocol version:</p> <ol style="list-style-type: none"> Stop VCS monitoring of the standby SM. Use the following VCS CLU command from /opt/VRTSvcs/bin: <code>#./hastop -local</code> Change the replication protocol. On the standby SM, run the following CLU command: <code>-bash-3.1\$ p3db --upgrade-rep-protocol</code> Restart VCS monitoring. From the /opt/VRTSvcs/bin folder, run the following VCS CLU command: <code>#./hastart</code> VCS monitoring starts the SM process automatically in the initialization state. Use the p3cluster CLU command to set the SM to the standby state: <code>-bash-3.1\$ p3cluster --standby</code> 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. Run the following VCS CLU command from /opt/VRTSvcs/bin: <code># hagrps -switch service group name -to System</code> Repeat Step a. to Step f. on the new standby SM. 	<p><i>Perform this operation after both the SMs are upgraded.</i></p> <p>Run the commands described in this step as the <i>admin</i> user on <i>both</i> the machines to upgrade the database replication protocol version.</p> <p>The p3db --upgrade-rep-protocol CLU command performs the following actions:</p> <ul style="list-style-type: none"> Removes the DB security flag Stops the SM Restarts the DB daemon Starts the SM Starts SM replication <p>For more information about the hagrps command, refer to your Veritas Cluster Server documentation.</p>
Step 17	<p>Add a user for PRPC authentication using the p3rpc CLU, for example:</p> <pre>-bash-3.1\$ p3rpc --set-user --username=username --password=password --remote=OTHER_SM_IP[:port]</pre>	<p>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.</p>
Step 18	<p>Configure the Cisco SCE platforms.</p>	<p>If you have a cascade SCE setup, configure the cascade SCE pair in the p3sm.cfg file. For details, see the <i>Cisco Service Control Management Suite Subscriber Manager User Guide</i>.</p>
Step 19	<p>Remove the dummy subscribers.</p> <p>On the new active SM, run the following CLU:</p> <pre>-bash-3.1\$ p3subs --remove -subscriber=first dummy subscriber name -bash-3.1\$ p3subs --remove -subscriber=second dummy subscriber name</pre>	<p>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.</p>

Migrating 4.1.x Subscriber Manager Data to 5.0.x

This section describes the procedure to migrate the Subscriber Manager data from Version 4.1.x to Version 5.0.x.

Step 1 Export the subscriber database in 4.1.x Subscriber Manager by running the p3subsdb CLU.

```
-bash-3.1$ p3subsdb --export --output=output filename
```

Step 2 Import the subscribers back into the database in 5.0.x Subscriber Manager by running the p3subsdb CLU.

```
-bash-3.1$ p3subsdb --import --file=file name from Step 1
```



Note

Ensure that the ~pcube/sm/server/root/ssu/subaware.pro file must be same as Step 1 and Step 2.

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 Cisco Service Control 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 Cisco Service Control Collection Manager, Release 5.0.x from Cisco Service Control Collection Manager, Releases 4.0.x and 4.1.x. To upgrade to Release 5.0.x from a version earlier than 3.8.5, you must first upgrade to version 4.0.x or 4.1.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 5.0.x

Step 1 Get the Cisco Service Control 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 Cisco Service Control Collection Manager server:

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

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

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

Step 5 (Optional) Enable verbose mode:

```
Do you want to enable verbose mode (for detailed installation) (yes/no)[no]:
```

Step 6 (Optional) Upgrade the Cisco Service Control Collection Manager tables to the latest schema:

```
Do you want to upgrade the CM Tables to latest Schema? (It will take time if the table have huge data)
(yes/no) [yes]:
```



Note

If you select the no option, run the `~scmscm/scripts/ upgradeRDRTTables.sh` as a `scmscm` user before manually starting Cisco Service Control Collection Manager. After the table upgrade, when Cisco Service Control Collection Manager comes up for the first time, the database tables that are new are created automatically.

Step 7 (Optional) Start the Cisco Service Control Collection Manager:

```
Would you like to start CM now? (yes/no) [yes]: yes
```



Note

If you enter no, manually start the Cisco Service Control Collection Manager using the `~scmscm/cm/bin/cm start` command.



Note

The `~scmscm/cm/config/apps/scasbb/latest/dbtables.xml` file is backed up in the same folder. The latest XML file is used for the Collection Manager process. To retain any configuration from earlier release, you must update the file manually.

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 Collection Manager is operational. If it 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.

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:

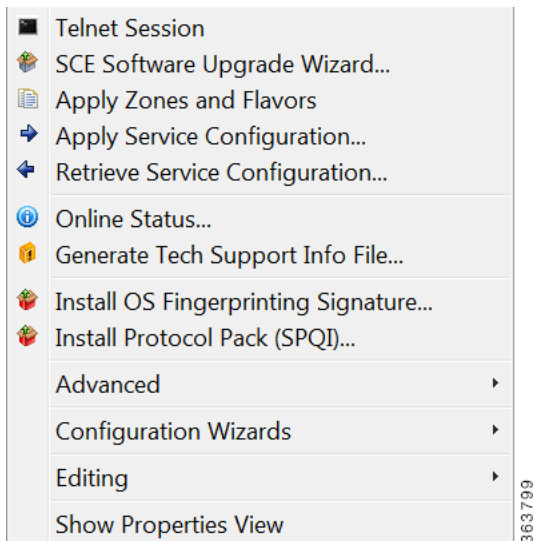
- If the IP address of all SCE platforms to be upgraded are not defined in the Network Navigator, gather the IP addresses of all SCE platforms to be upgraded.
- Download the relevant pkg file, pqi file, and protocol pack to a local location or to a location accessible by FTP. If using an FTP site, make 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](#)).

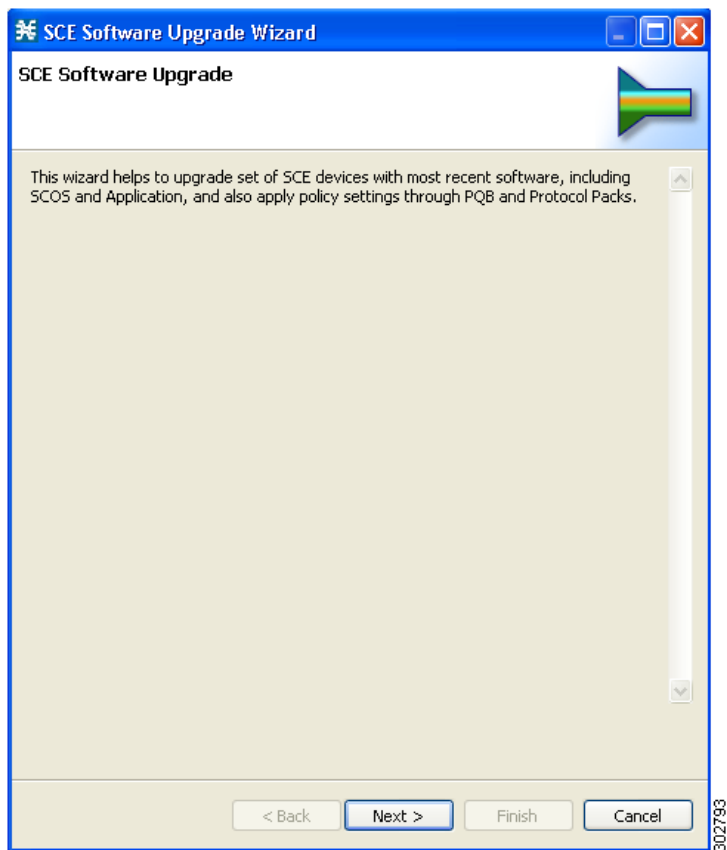
If the Cisco SCE platforms are not yet defined in the Network Navigator, you can select the site node.

Figure 1 *Network Navigator*



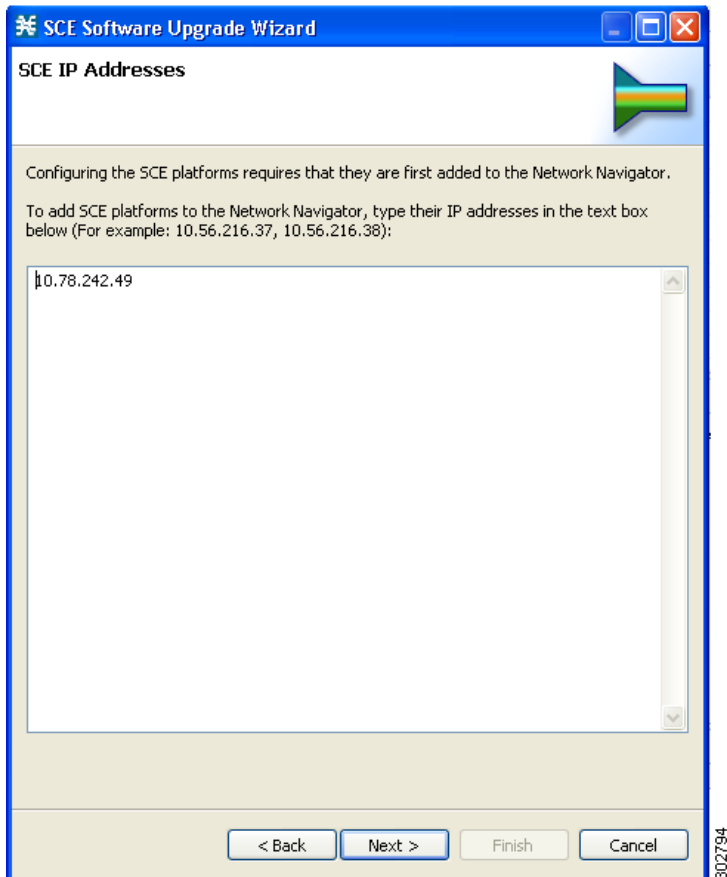
The SCE Software Upgrade Wizard opens. Click **Next** (see [Figure 2](#)).

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

SCE Software Upgrade Wizard

SCE Usernames and Passwords

A password for the SCE 10.78.248.168 is missing

In order to connect to the SCE platforms, a username and a password need to be specified for each SCE.

☒ Use a common username and a common password for all SCE platforms:

Username:

Password:

PRPC Port:

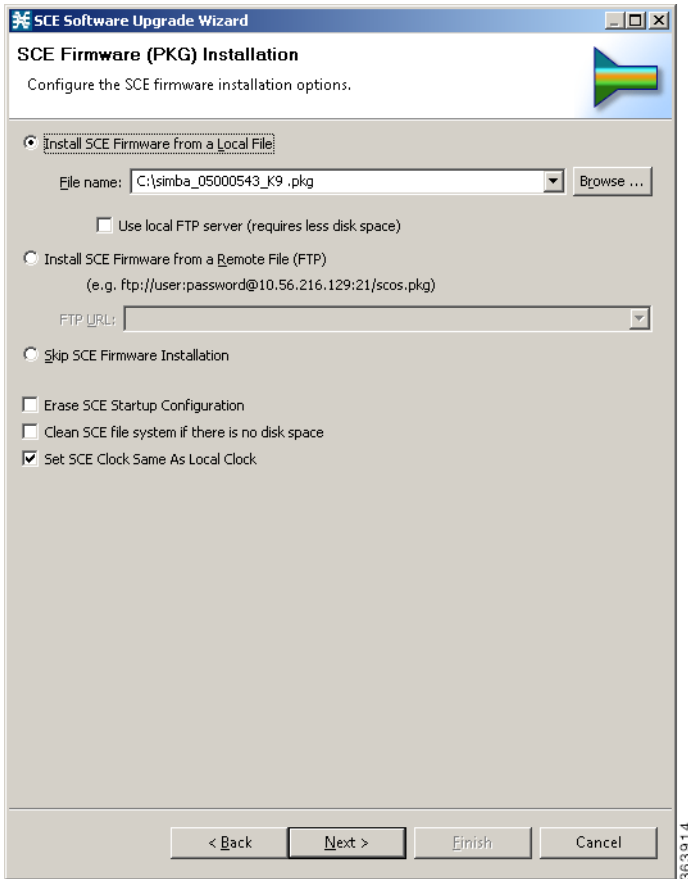
☐ Use separate usernames and passwords for each SCE platform:

SCE IP Address	Username	Password	PRPCPort
10.78.248.168	admin		14374

< Back Next > Finish Cancel

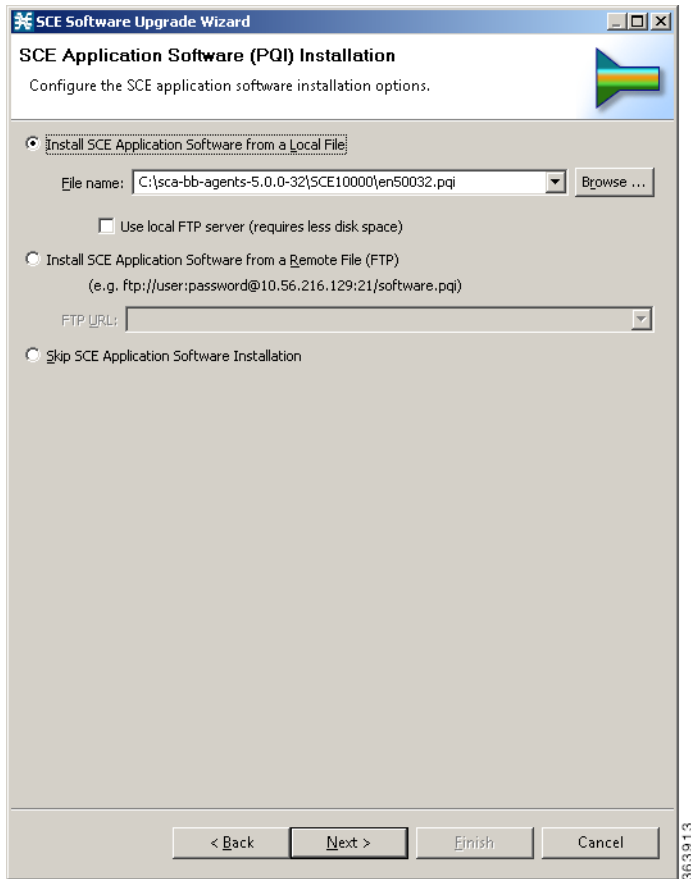
Step 4 In the SCE Firmware (PKG) Installation pane (see [Figure 5](#)), specify the location of the firmware file to be installed on all the selected Cisco SCE platforms and click **Next**.

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



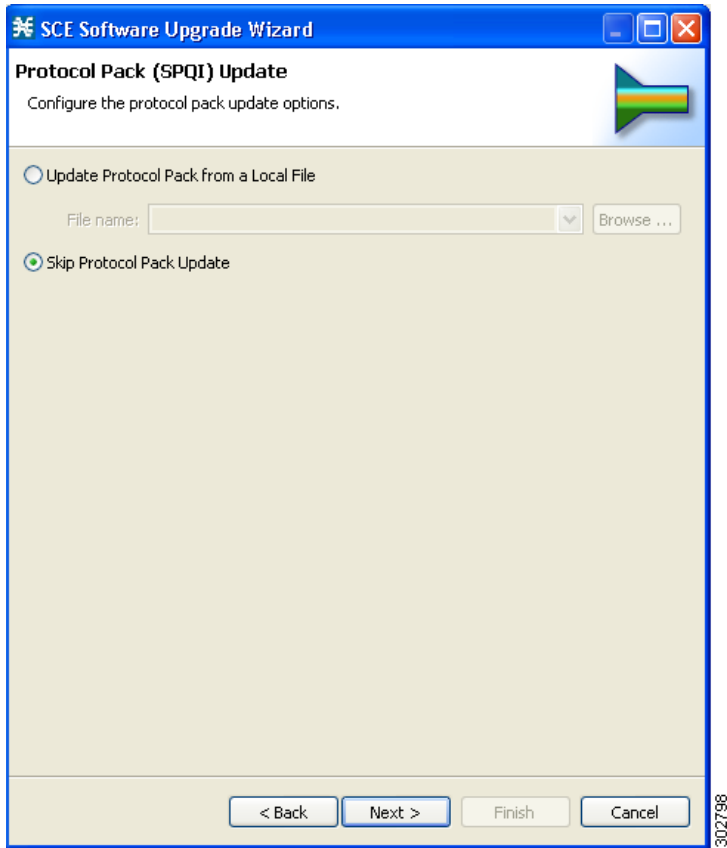
Step 6 In the Protocol Pack (SPQI) Update pane (see [Figure 7](#)), check Skip Protocol Pack Update and click **Next**.



Note

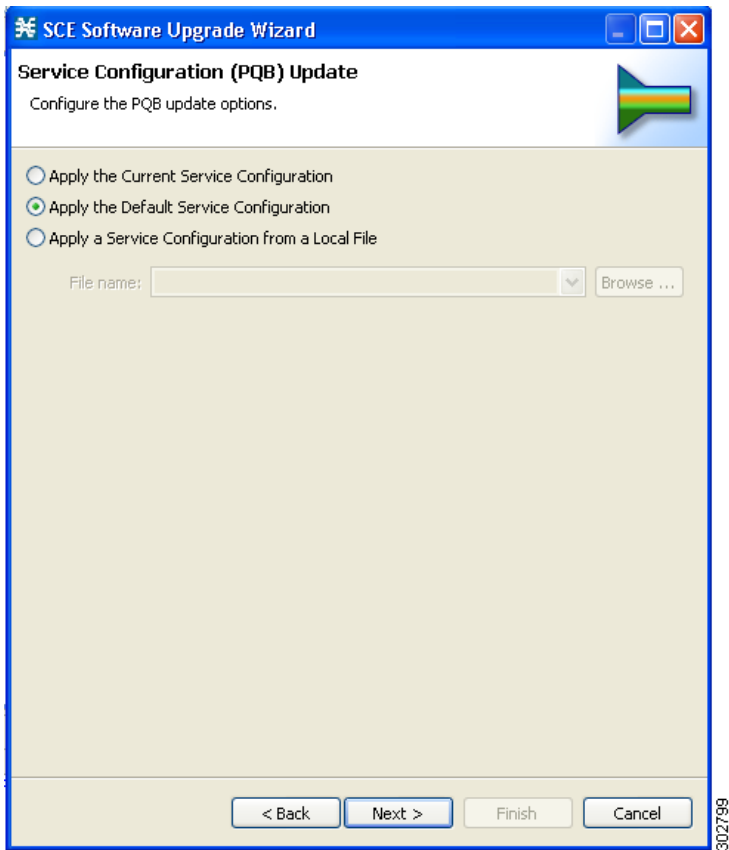
If you install the protocol pack during the upgrade, it must be the same version or a later version of the protocol pack you are upgrading from.

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



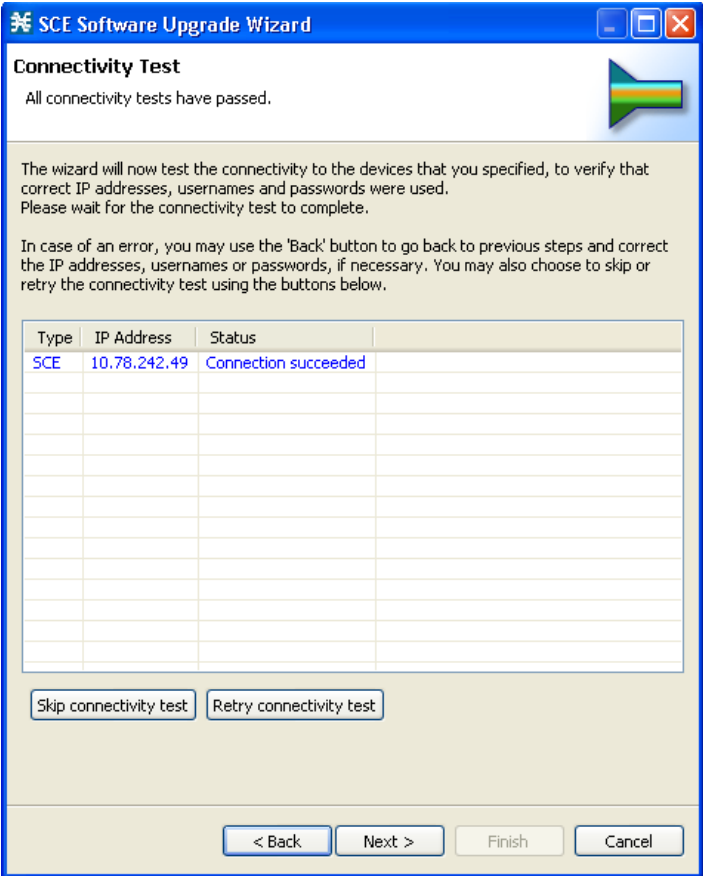
Step 8 The Connectivity Test pane of the SCE Software Upgrade Wizard is displayed (see [Figure 9](#)). Click **Next**.



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**.

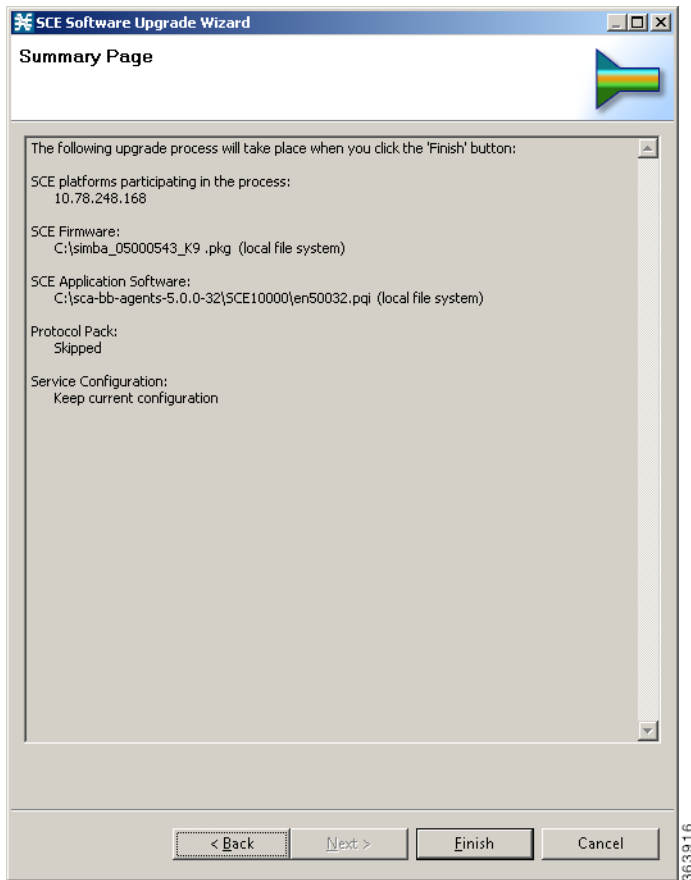
Figure 9 **Connectivity Test**



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):

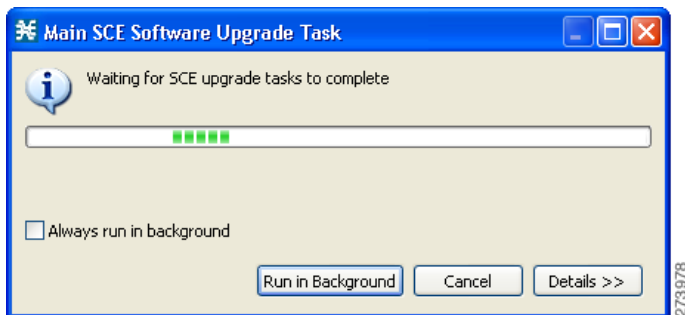
- Retrieve the current service configuration from the SCE platform (only if the current service configuration is going to be reinstalled after the upgrade).
- Uninstall the existing application software (PQI).
- Upgrade SCE platform firmware (PKG).
- Install application software (PQI).
- Apply service 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](#)).

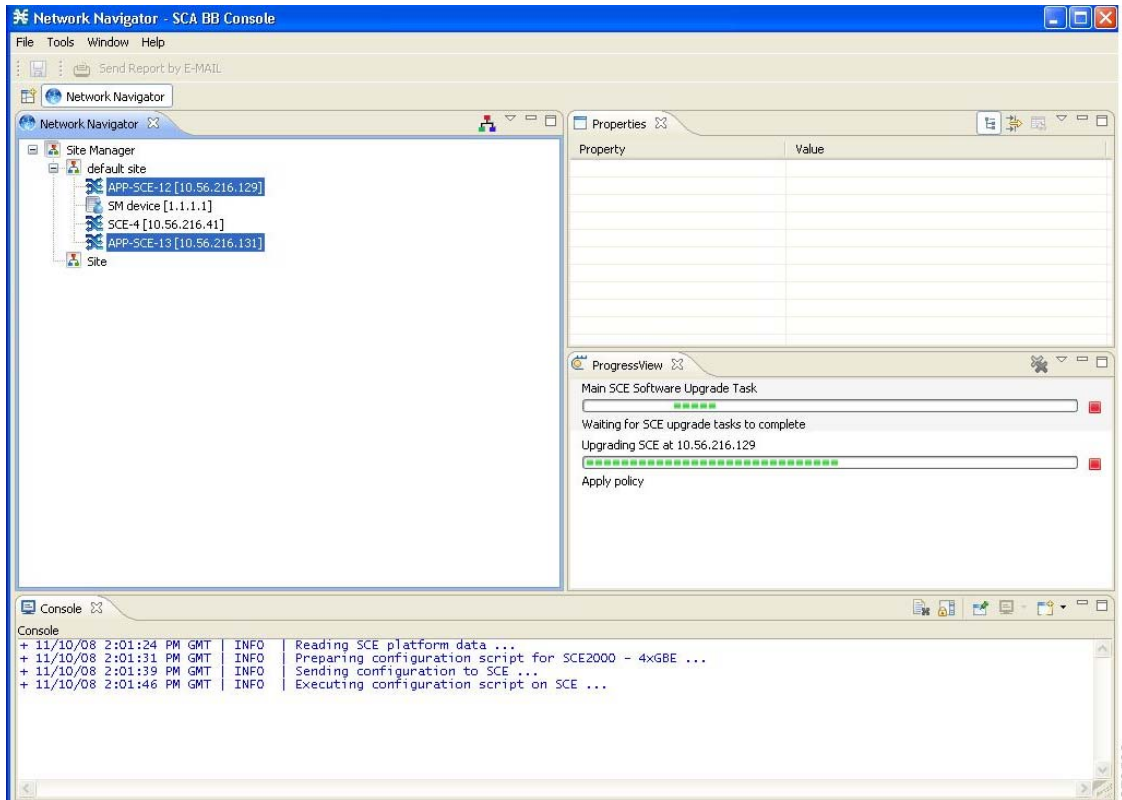
Click **Run in Background** to run the upgrade in the background.

Figure 11 *Main SCE Software Upgrade Task*



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

Figure 12 *Network Navigator*



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 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 because of misclassification of traffic flows that were initiated before upgrade completion. See the [“Misclassification of Flows Initiated Before 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 and Subscriber Manager GUI is not backward compatible and can work only with the 4.1.x system components (SCE platform, Collection Manager, and Subscriber Manager).

Cisco SCA BB Console Interoperability

Version 4.1.x of the Network Navigator cannot apply service configurations to earlier versions of the SCE platforms. Nevertheless, the Network Navigator 4.1.x can upgrade the SCE platform to 4.1.x, and then service configurations can be applied.

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.

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

Configuration

When upgrading the Collection Manager to Version 5.0.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.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved



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.