



Cisco Service Control Guide to Upgrading to SCA BB 3.1 from SCA BB 3.0

Release 3.1
May 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0501R)

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.

Cisco Service Control Guide to Upgrading to SCA BB 3.1 from SCA BB 3.0
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

General 1-1

- Purpose and Scope 1-1
- Document Outline 1-1
- References 1-2

CHAPTER 2

Supported Upgrade Use Cases 2-1

- Upgrade Use Cases 2-1

CHAPTER 3

Upgrade Objectives and Limitations 4-1

- Upgrade Objectives 4-1
- Supported Working Configurations 4-2
- SCE Platform 4-2
 - Upgrade Procedure Limitations 4-2
 - Link Downtime Due to LIC Re-Burning 4-2
 - Misclassification of Flows Initiated Prior to Upgrade Completion 4-2
 - Service Downtime 4-2
 - Loss of Aggregated Unreported Data 4-3
 - Loss of Configuration 4-3
- SCA BB Clients and Service Configuration 4-3
 - Upgrade Procedure Limitations 4-3
 - SCA BB Console Interoperability 4-3
 - Service Configuration Upgrade 4-4
 - User Defined Signatures 4-4
 - Reporter and DB Interoperability 4-4
 - Running Two SCA BB Consoles or Reporters 4-4
- Subscriber Manager 4-4
 - Upgrade Procedure Limitations 4-4
- LEG Configuration 4-4
- Quota Manager 4-5
- Collection Manager 4-5
 - Upgrade Procedure Limitations 4-5
 - Configuration 4-5

Rollback Procedure 4-5

CHAPTER 4

Upgrade Procedure 7

Upgrading from Version 3.0 to Version 3.1 7



CHAPTER 1

General

This module gives an overview of the Solution Upgrade from SCA BB 3.0 to SCA BB 3.1

Upgrading the Cisco Service Control solution is a complicated task due to the need to upgrade the software release on several network elements, while maintaining data and keeping the downtime to a minimum. Therefore, this process requires careful design and preparation. This document provides a blueprint for the upgrade process, as well as limitations and issues to consider, to be used while designing the upgrade process for a specific deployment.

- [Purpose and Scope](#)
- [Document Outline](#)
- [References](#)

Purpose and Scope

This document describes how to upgrade an existing installation of the Cisco Service Control solution to SCA BB 3.1. It provides an overview of the overall solution upgrade procedure, as well as the limitations of this procedure.

For detailed instructions of the upgrade procedure for each solution component, see the [References](#) section.

This document describes the simple approach to upgrading and the limitations imposed by it. In some cases, an approach may need to be adapted to address specific requirements.

Document Outline

The “[Supported Upgrade Use Cases](#)” module describes the service control deployments to which this document applies.

The “[Supported Working Configurations](#)” module describes the objectives and the limitations of the upgrade process.

The “[Upgrade Procedure](#)” module describes the step by step upgrade procedure.

References

The following documents provide detailed information about the upgrade procedures for the solution components:

- SCOS upgrade procedure:
 - See “Upgrading SCE Platform Firmware” in the “Operations” chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*
- SCA BB upgrade procedure:
 - See “Upgrading SCA BB” in the “Getting Started” chapter of the *Cisco Service Control Application for Broadband User Guide*
- Subscriber Manager upgrade procedure:
 - See “Upgrading the Subscriber Manager” in the “Installation and Upgrading” chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*
- Collection Manager upgrade procedure:
 - See “Upgrading to CM Version 3.1” in the “Installing the Collection Manager and Getting Started” chapter of the *Cisco Service Control Management Suite Collection Manager User Guide*



CHAPTER 2

Supported Upgrade Use Cases

This module describes the supported upgrade use cases.

All references are to a deployment where a single CM and a single SM cluster are deployed with one or more SCE platforms. If a deployment is composed of several CMs and SMs, then each SCE platform group communicating with a single CM and SM should be considered as a separate deployment for the purposes of the upgrade procedure.

Upgrade Use Cases

The following upgrade use case is supported. The exact description, procedures, and limitations for this use case are described in the following sections.

- Upgrade from SCA BB 3.0 to SCA BB 3.1

The upgrade procedures that are described refer to a use case where all solution components (SCE platform, CM, and SM) exist. If one of the components is not in use (no Collection Manager or no Subscriber Manager), then the corresponding phase in the upgrade procedure should be skipped.



CHAPTER 3

Upgrade Objectives and Limitations

This module compares the objectives of the upgrade procedure with the limitations that can be expected for each component throughout this process.

- [Upgrade Objectives](#)
- [Supported Working Configurations](#)
- [SCE Platform](#)
- [SCA BB Clients and Service Configuration](#)
- [Subscriber Manager](#)
- [Collection Manager](#)
- [Rollback Procedure](#)

Upgrade Objectives

Generally, upgrade procedures aim for the following objectives for the entire solution:

- No loss of configuration
- No loss of data
- No network downtime
- Minimal or no service downtime
- Safe rollback
- Upgrade modularity
- Functional equivalency
- Upgrade verification

Some of these objectives are achieved through maintaining interface compatibility; for example, CSV files, RDRs, DB schemes, and CLI retain compatibility. Programmable interfaces retain binary compatibility or interface compatibility (for static C linking).

Not all requirements are met on each perspective of the solution. Limitations with respect to these objectives are mentioned in the following sections and in the relevant component manuals.

Supported Working Configurations

The SCA BB 3.1 solution supports a combination of component versions:

- SCOS 3.1.
- Application - SCA BB 3.1 (PQIs for installation on SCE platform and SCMS-SM).
- SCMS-SM 3.1 (if an SM is required for the deployment).
- SCMS-CM 3.1 or 3.0 (if a CM is required for the deployment).

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

SCE Platform

Upgrade Procedure Limitations

- [Link Downtime Due to LIC Re-Burning](#)
- [Misclassification of Flows Initiated Prior to Upgrade Completion](#)
- [Service Downtime](#)
- [Loss of Aggregated Unreported Data](#)
- [Loss of Configuration](#)

Link Downtime Due to LIC Re-Burning

When upgrading from 3.0.0 only: Link downtime is expected during SCE platform upgrade (the LIC chip firmware is reburned). The expected downtime depends on the system's auto-negotiation configuration, and can be up to one minute.

Misclassification of Flows Initiated Prior to Upgrade Completion

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

Service Downtime

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

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

Loss of Aggregated Unreported Data

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

This is true also for High Availability configurations.

Loss of Configuration

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

SCA BB Clients and Service Configuration

SCA BB Console, which incorporates the service configuration editor, SM GUI, and Reporter, is not backward compatible and can work only with the 3.1 system components (SCE platform, CM, SM).

Upgrade Procedure Limitations

- [SCA BB Console Interoperability](#)
- [Service Configuration Upgrade](#)
- [User Defined Signatures](#)
- [Reporter and DB Interoperability](#)
- [Running Two SCA BB Consoles or Reporters](#)

SCA BB Console Interoperability

Version 3.1 of the Network Navigator cannot apply service configurations to version 3.0 SCE platforms. Nevertheless, the Network Navigator 3.1 can upgrade the SCE to 3.1, and then service configurations can be applied.

Service Configuration Upgrade

Older Service Configuration files need to be adapted to SCA BB 3.1 prior to applying them to the upgraded system. This can be done in one of two ways:

- Re-implement the Service Configuration using the SCA BB 3.1 Service Configuration Editor
- Port the old configuration to SCA BB 3.1 semantics by opening it with the SCA BB 3.1 Service Configuration Editor. In this case, it is recommended to follow the SCA BB user guide description of the default 3.1 configuration, to allow incorporating 3.1 enhancements.

User Defined Signatures

If you created a DSS in the Signature Editor and want to install a protocol pack, you need to merge the DSS with the signatures in the protocol pack by performing the following general steps:

- Extract the DSS from the protocol pack.
- Open your DSS and import the protocol pack DSS into the signature editor and ensure there are no overlapping signature IDs.
- Save the merged DSS.

Reporter and DB Interoperability

The Reporter and Reporter Templates of 3.1 can be used to create reports from a 3.0 database provided that the same reports existed in 3.0. However, reports that are new in 3.1 cannot be created when connecting to a 3.0 database.

Running Two SCA BB Consoles or Reporters

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

Subscriber Manager

- [Upgrade Procedure Limitations](#)
- [LEG Configuration](#)
- [Quota Manager](#)

Upgrade Procedure Limitations

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

LEG Configuration

The configuration of the SM LEGs is lost during the upgrade. Follow the upgrade procedure of the SM LEGs in the relevant reference guide.

Quota Manager

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

Collection Manager

- [Upgrade Procedure Limitations](#)
- [Configuration](#)

Upgrade Procedure Limitations

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).

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

Configuration

When upgrading the CM from 3.0.5 or 3.0.6 to 3.1, the users configuration on the CM server (the PRPC users file, prpc.usr) is deleted. It is necessary to redefine the users after the upgrade is completed.

Rollback Procedure

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

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

**Note**

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



CHAPTER 4

Upgrade Procedure

This module details the upgrade procedure for upgrading from a functional SCA BB 3.0 deployment to SCA BB 3.1.

This is a high level description of the procedure. The specific details are found in the corresponding user manuals.

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

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

Upgrading from Version 3.0 to Version 3.1

SUMMARY STEPS

1. Upgrade the SM (or SM cluster) according to the procedure described in the SM user manual
2. Deploy or upgrade the CM to 3.1
3. Upgrade the SCE platform software (SCOS and application PQI).
4. Remove the second CM running the former version (if one was used) once the upgrade of all SCE platforms is complete.

DETAILED STEPS

-
- Step 1** Upgrade the SM (or SM cluster) according to the procedure described in the SM user manual
- a. Uninstall the SCA BB application and the SM LEGs' PQIs
 - b. Run the SM upgrade script.
 - c. Install the SCA BB application and the SM LEGs' PQIs.
 - d. Configure the SCE cascade to the SM as described in the *Cisco SCMS Subscriber Manager User Guide* .

This step is required because in version 3.1, the SM is aware of SCE cascade topologies and must be configured accordingly. Immediately after the upgrade, all SCEs are configured to the SM as standalone SCEs. You must configure the SCEs manually after the upgrade of an SCE pair.

- e. Configure the cascade SCEs as a cascade pair in the SM configuration.

This causes the SM to treat the standby SCE that will be upgraded to 3.1.0 in the correct way and not send subscriber updates to it.

The SM will not update an SCE that is identified as standby even if it is configured as 'standalone' in the SM.

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

Step 2 Deploy or upgrade the CM to 3.1

- In the case of deployment of an additional CM and database for the transition phase (*two CM databases* in total, regardless of whether or not the configuration is bundled), collection will work for all SCE platforms (both the older version and 3.1). Regarding *non-bundled databases*, there may be several ways to implement this; it is recommended to consult a DB specialist if you are using a non-bundled database.
 - Each CM collects RDRs from a single version, to a distinct database (either bundled or non-bundled) and CSV repository.

Step 3 Upgrade the SCE platform software (SCOS and application PQI).

This also applies in the case of an SCE platform cluster. See the *SCE Installation Guide* and the *Software Configuration Guide* for more details.

The SCE platform upgrade procedure involves the following high-level steps:

- Retrieve the service configuration (PQB)—Use a 3.0 SCA BB Console.
- Update the service configuration to 3.1—Open the old service configuration in the Service Configuration Editor in the new Console, and make any necessary adjustments to the old service configuration. These changes are described in the *SCA BB 3.1 Release Notes*. Alternatively, create a new service configuration using the 3.1 Service Configuration Editor.
- Use the 3.1 Network Navigator GUI to install SCOS 3.1—Install PQI 3.1 on the SCE platform and then install the latest protocol pack on top of SCA BB 3.1.
- Apply the service configuration to the SCE platform.
 - Each SCE platform remains functional from a traffic control perspective from the completion of the SM upgrade until it is upgraded, and then again after the upgrade. On High Availability configurations, no service downtime is expected as the SCE upgrade is performed when the SCE is in standby mode.
 - Make sure the upgraded SCE platform RDRs are directed to the CM running version 3.1. Service downtime (from a collection perspective) depends on the CM configuration that you have implemented (single or dual during the upgrade).

For a cascade SCE pair:

- Verify that the SM was already upgraded to 3.1.
- Upgrade the standby SCE as described above.
- Force a fail-over.
- Upgrade the new standby SCE (the formerly active SCE) as describe above.

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

- Step 4** Remove the second CM running the former version (if one was used) once the upgrade of all SCE platforms is complete.
-

