



# Release Notes for Cisco Service Control Application for Broadband, Release 3.7.x

---

Revised: March 28, 2012, OL-24158-06



Note

---

This document supports all 3.7.x releases.

---

## Overview

The release notes for Cisco Service Control Application for Broadband (SCA BB) describe the enhancements provided in Cisco SCA BB Release 3.7.5, Cisco SCA BB Release 3.7.2, Cisco SCA BB Release 3.7.1, and Cisco SCA BB Release 3.7.0. These release notes are updated as needed.

For a list of caveats that are applicable to Cisco SCA BB Release 3.7.5, see the [“Open Caveats, Release 3.7.5” section on page 6](#).

For a list of caveats that are applicable to Cisco SCA BB Release 3.7.2, see the [“Open Caveats, Release 3.7.2” section on page 8](#).

For a list of caveats that are applicable to Cisco SCA BB Release 3.7.1, see the [“Open Caveats, Release 3.7.1” section on page 9](#). Also, if you are upgrading Cisco SCE 2000 to Release 3.7.1, see this section for important information about capacity degradation.

For a list of caveats that are applicable to Cisco SCA BB Release 3.7.0, see the [“Open Caveats, Release 3.7.0” section on page 22](#).

For information about the features that were added and issues that were resolved in the Release 3.6.x train, see:

- [Release Notes for Cisco Service Control Application for Broadband \(SCA BB\), Release 3.6.x](#)

For information about the features that were added and issues that were resolved in the Release 3.5.x train, see:

- [Release Notes for Cisco Service Control Application for Broadband \(SCA BB\), Release 3.5.5](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

For information about the features that were added and issues that were resolved in the Release 3.1.x train, see:

- [Release Notes for Cisco Service Control Application for Broadband \(SCA BB\), Release 3.1.7](#)

For information about new and improved protocol signatures for Cisco SCA BB, see:

- [Release Notes for Cisco Service Control Application for Broadband \(SCA BB\) Protocol Packs Notes](#)

For further information about related products, see the latest versions of the following release notes:

- [Release Notes for Cisco Service Control Operating System \(SCOS\)](#)
- [Release Notes for Cisco Service Control Management Suite Subscriber Manager \(SCMS SM\)](#)
- [Release Notes for Cisco Service Control Management Suite Collection Manager \(SCMS CM\)](#)

For the compatibility matrix, see the *Cisco Service Control Application for Broadband Download Guide*.

## Contents

- [Introduction, page 3](#)
- [Cisco Service Control Application for Broadband Release 3.7.5, page 4](#)
- [Cisco Service Control Application for Broadband Release 3.7.5, page 4](#)
- [Cisco Service Control Application for Broadband Release 3.7.1, page 9](#)
- [Cisco Service Control Application for Broadband Release 3.7.0, page 20](#)
- [Obtaining Documentation and Submitting a Service Request, page 31](#)

## Introduction

This document assumes that the reader has a good working knowledge of the Cisco Service Control solution. For additional information, see the Cisco SCA BB documentation.

To access the online Cisco Service Control documentation site, follow these instructions:

1. On Cisco.com, go to the following page:  
<http://www.cisco.com/cisco/web/psa/default.html?mode=prod>
2. Choose **Products > Service Exchange > Cisco Service Control > Cisco Service Control Application Suite > Cisco Service Control Application for Broadband**.

# Cisco Service Control Application for Broadband Release 3.7.5

This section describes the new protocol support, and resolved and open issues pertaining to Cisco SCA BB Release 3.7.5.

- [New Features, page 4](#)
- [Protocol Support, page 4](#)
- [Resolved Caveats, Release 3.7.5, page 4](#)
- [Open Caveats, Release 3.7.5, page 6](#)

## New Features

Cisco SCA BB Release 3.7.5 introduces IPv6 phase 1.

## Protocol Support

Protocol Pack #27 is included in Cisco SCA BB Release 3.7.5. For details on the protocols support, see the *Cisco Service Control Application for Broadband Protocol Pack Notes* and the *Cisco Service Control Application for Broadband Reference Guide, Release 3.7.x*.

## Resolved Caveats, Release 3.7.5

This section describes the resolved caveats in Cisco SCA BB Release 3.7.5 that relate to the general issues pertaining to the Cisco SCA BB Console.

### **CSCsy96654**

When an attack was detected while setting an attack detector to block a specific TCP port, the block rule was applied for all the TCP ports other than the port for which the attack detector was defined.

This issue is resolved.

### **CSCtj19964**

In the Cisco SCA BB Console, when the Generate the Virtual Links Usage RDRs check box was unchecked, Virtual Link Usage RDRs were generated until the VLink Mode Enable setting was disabled.

This issue is resolved.

### **CSCtj49052**

In the Network Navigator tab of the Cisco SCA BB Console, when users right-clicked the corresponding SCE device and selected the Online Status option, the bandwidth value of the SCE device was displayed as a negative value.

This issue is resolved.

**CSCts52096**

In the Edit Subscriber window, the Subscriber Package drop-down list contained a blank space between the each package ID.

This issue is resolved.

**CSCts97290**

in the Quota Bucket Profile Editor window, due to low resolution, users were not able to transfer services between the Services tab and the Time frame tabs because the buttons with arrow were not visible.

This issue is resolved.

**CSCtx07240**

When the virtual channels for virtual links were created through the CLI, duplicate CLIs were created in the configuration file.

This issue is resolved.

**CSCtx48424**

From the Cisco SCA BB Console, when a default virtual link value was set for a newly added global controller under the virtual links, it failed in the downstream direction.

This issue is resolved.

**CSCtx48498**

After the peak information rate (PIR) value for a virtual link was configured, the default value was reset automatically when the corresponding virtual link was reloaded.

This issue is resolved.

**CSCtx95224**

The authorised users were unable to import the sce-url-database.

This issue is resolved.

## Open Caveats, Release 3.7.5

This section describes the open caveats in Cisco SCA BB Release 3.7.5.

### CSCtq80422

In the Cable Modem Termination System (CMTS), when the Virtual Link Manager (VLM) in the vlink.cfg file of the Cisco Subscriber Manger is enabled, all the virtual links in the CMTS do not get provisioned from the Subscriber Manager to Cisco SCE.

#### Workaround:

No known workaround.

### CSCty73869

After enabling the virtual link mode, when a virtual link was created manually using the **virtual-links index <index> name <name> direction [upstream | downstream]** command, and a policy applied from Cisco SCA BB with the **Keep Virtual Link rate limits unchanged** button selected, the policy did not get applied and some of the virtual links were getting deleted.

#### Workaround:

After enabling the virtual link mode, when a virtual link is manually created using the **virtual-links index <index> name <name> direction [upstream | downstream]** command, ensure that you create a virtual channel index for the corresponding virtual link using the **virtual-links channel index <index> name <name> parent-virtual-link index <index> direction [upstream | downstream]** command.

## Cisco Service Control Application for Broadband Release 3.7.2

From March 28, 2012, a new version of the Cisco SCA BB Release 3.7.2 is available on Cisco.com. This version of Cisco SCA BB addresses the following issues:

- CSCtx33874—Cisco SCA BB Release 3.7.2 failed to apply policies on Cisco SCE 8000, running Cisco SCOS Release 3.7.2.
- CSCtx48102—After reloading the Cisco SCE devices, the SPQI was removed from the device.
- CSCtx48102—After reloading the Cisco SCE devices, the startup-config-application was not saved.
- CSCtx48102—While reloading an Cisco SCE device, the device started in the transparent mode.

We recommend that you download and install the latest version of the application. If you have installed Cisco SCA BB Release 3.7.2(build 426), uninstall it before you install the latest version. After installing the new version, confirm that the application build number is 434.

This section describes the new protocol support, and resolved and open issues of Cisco SCA BB, Release 3.7.2:

- [New Features, page 7](#)
- [Protocol Support, page 7](#)
- [Resolved Caveats, Release 3.7.2, page 7](#)
- [Open Caveats, Release 3.7.2, page 8](#)

## New Features

Cisco SCA BB Release 3.7.2 introduces the Border Gateway Protocol (BGP) Autonomous System Dynamic Detection feature.

## Protocol Support

Protocol Pack #25 is included in Cisco SCA BB Release 3.7.2. For details on the protocols supported, see the *Cisco Service Control Application for Broadband Protocol Pack Notes* and the *Cisco Service Control Application for Broadband Reference Guide, Release 3.7.x*.

**Note**

---

When you upgrade old PQB files, new signature-based protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as *Default Service*. To resolve this issue, manually assign these protocols to a service.

---

## Resolved Caveats, Release 3.7.2

This section describes the resolved caveats in Cisco SCA BB Release 3.7.2 that relate to the general issues pertaining to the Cisco SCA BB Console.

**CSCtu23698**

On the SCE 8000 10GBE device running Cisco SCOS Release 3.6.5 or later, Cisco SCA BB failed to create more than 1024 global controllers for upstream and downstream directions.

This issue is resolved.

**CSCtu04633**

Cisco SCA BB failed to modify the subscriber attributes from Cisco SCA BB console when custom properties were configured in the Cisco SCMS Subscriber Manager.

This issue is resolved.

**CSCtw85408**

Cisco SCA BB failed to import the Dynamic Signature Script (DSS) file created using the Cisco SCA BB Signature Editor page.

This issue is resolved.

## Open Caveats, Release 3.7.2

This section describes the open caveats in Cisco SCA BB Release 3.7.2.

### **CSCtu20333**

The script to fetch BGP Autonomous System information takes only one router IP address as input.

#### **Workaround:**

Modify the IP address in the properties file and run the script separately for each router IP address.

### **CSCtu21238**

The script to fetch BGP Autonomous System information fails to generate the CSV file in Linux environment.

#### **Workaround:**

No known workaround.



# Cisco Service Control Application for Broadband Release 3.7.1

This section describes the new protocol support, and resolved and open issues of Cisco SCA BB, Release 3.7.1:

- [Protocol Support, page 9](#)
- [Resolved Caveats, Release 3.7.1, page 9](#)
- [Open Caveats, Release 3.7.1, page 9](#)

## Protocol Support

Protocol Pack #25 is included in Cisco SCA BB Release 3.7.1. For details on the Protocols supported, see the *Protocol Pack Notes* and the *Cisco Service Control Application for Broadband Reference Guide, Release 3.7.x*.

**Note**

When you upgrade old PQB files, new signature-based protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as *Default Service*. To resolve this issue, manually assign these protocols to a service.

## Resolved Caveats, Release 3.7.1

This section describes resolved caveats in Cisco SCA BB Release 3.7.1 that relate to the general issues concerning the Cisco SCA BB Console.

**CSCtr66698**

Cannot use asterisk (\*) as the value for a Zone; but can configure Default Zone. Default Zone displays asterisk as the value.

This issue is resolved.

**CSCtr47571**

Can not use tilde (~) as path prefix, host suffix, or path suffix when configuring Flavor in Cisco SCA BB 3.7.0.

This issue is resolved.

## Open Caveats, Release 3.7.1

This section describes the open caveats in Cisco SCA BB Release 3.7.1:

- [Protocol Pack, page 10](#)
- [Traffic Processing, page 10](#)
- [Cisco SCA BB Console, page 15](#)
- [Configuration Management, page 19](#)

## Protocol Pack

This section describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to Protocol Pack:

### **CSCtt70660**

A capacity degradation of 1.76 percentage is observed on Cisco SCE 8000 with SCE Release 3.7.1, when compared to Cisco SCE 8000 with SCE Release 3.7.0.

The fix for this issue will be available in future Protocol Pack releases.

#### **Workaround:**

No known workaround.

### **CSCts23380**

A capacity degradation of 5.02 percentage is observed on Cisco SCE 2000 with SCE Release 3.7.1, when compared to Cisco SCE 2000 with SCE Release 3.7.0.

The fix for this issue will be available in future Protocol Pack releases.

#### **Workaround:**

No known workaround.

## Traffic Processing

This section describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to traffic processing:

- [General, page 22](#)
- [Traffic Classification, page 24](#)
- [Traffic Accounting and Reporting, page 25](#)
- [Traffic Control, page 26](#)

### General

This section describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to general issues concerning traffic processing.

### **CSCtq12796**

In the Anonymous Group Manager GUI tool, the values for Template ID, Package ID, UpVlink, and DownVlink are restricted to 99. But in SCE, the values for Template ID and Package ID are restricted to 4999, and values for UpVlink, DownVlink are restricted to 1023. The values supported should be same in both the GUI and the SCE.

#### **Workaround:**

No known workaround.

**CSCtq12777**

Failed to connect to multiple Subscriber Managers by using the Subscriber Manager GUI in Cisco SCA BB Console.

When connected to a Subscriber Manager, if you try to connect to a second Subscriber Manager, the first Subscriber Manager gets replaced with the second Subscriber Manager.

**Workaround:**

No known workaround.

**CSCtq15400**

If two zeroes are added to a new Protocol ID to avoid ID duplication, the issue gets resolved only after two attempts. Also, even if you use a new ID in the second attempt, the ID you entered during the first attempt is saved.

For example, if the new Protocol ID is 4200, the first attempt fails. In the second attempt, even if you use a new ID (4211), 4200 is saved as the new Protocol ID.

**Workaround:**

If you use two zeroes, enter the same value during both the attempts.

**CSCsx75003**

The PQI installation process should reserve more disk space on SCE 2000.

The PQI installation process fails because of insufficient disk space on the SCE 2000. The SCE file system containing a lot of files consumes the disk space.

**Workaround:**

Manually remove the unnecessary files from the SCE file system.

**CSCsz59158**

The SCE 8000 MGBE might crash when you apply a PQB that contains 1000 global controllers.

If a policy with 1000 global controllers is not applied correctly after a reload, the SCE might run out of memory and the box may crash.

**Workaround:**

There is no known workaround.

**CSCtq99331**

When applying policies for different templates, if the virtual link is enabled, an error similar to this appears:

```
+ 6/16/11 5:41:17 PM IST | ERROR | Failed to apply service configuration at "SCE device
[10.78.241.106]": Error Code = 1, Description: "Input key should be number between 0 to
4,294,967,295More info: in func 'CmdLut::overwriteManyCfg',
lutName='GT_LUT_VIRTUAL_upLinkId2AppAGCIdx', key[0]='-65536', value[0]='0',
numVariables=3..", Detailed: "" (LUT_overwriteManyCfg:{key=[Ljava.lang.String;@21f572,
slot=0, lutName=GT_LUT_VIRTUAL_upLinkId2AppAGCIdx, value=[Ljava.lang.String;@21f579})
```

**Workaround:**

Disable the virtual link in SCE using the **no virtual link** CLU command before applying the new configuration.

## Traffic Classification

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to traffic classification.

### CSCsd81077

The same flow can be classified into different services, depending on a zone configuration that seems unrelated. This occurs after you define a new port-based protocol and then create a new service, adding a service element with the new protocol and a non-default zone to the service. Flows that match the new protocol but do not match the zone of the service element are now mapped to the Default Service.

Complete these steps (The unexpected flow classification occurs at step 6):

1. Add a new port-based protocol. For example, doom2 on TCP port 6666. Do not add the protocol to any service.
2. The SCE now classifies flows that match the doom2 protocol (TCP on port 6666) as Generic TCP, as expected.
3. Add a zone named gaming servers.
4. Create a new service called doom2 gaming servers. Add a service element, where the Protocol is doom2 and the Zone is gaming servers.
5. The SCE now classifies flows that match the doom2 protocol and the gaming servers zone to the new doom2 gaming servers service, as expected.
6. However, flows that match the doom2 protocols, but *do not* match the gaming servers zone, is classified as Default Service instead of Generic TCP.
7. If you delete the doom2 gaming servers service, the same flows that were classified as Default Service, is again classified (correctly) as Generic TCP.

### Workaround:

Add the service element <New port-based protocol, Initiated by either side, \*, \*> to an existing service. (You can also define a new service for this purpose.) After you do that, transactions using the specific protocol but with network IP addresses that do not match the specific zone, go to the less specific service.

For the example given above, add the service element <doom2, Initiated by either side, \*, \*> to the Generic TCP service.

### CSCsi46655

When SCA BB is deployed in an environment where it is required to analyze traffic in VLANs/VPNs with overlapping IP addresses, some of its capabilities, which rely on uniqueness of IP addresses in the network, do not function:

- Classification—No support for zones.
- Reporting—Reports based on IP addresses in Transaction RDRs are not accurate.

Many reports in the following categories rely on IP uniqueness:

- Mail and News
- Traffic Discovery—Statistics
- Web and Streaming

- Protocol Library—Mechanism based on IP addresses. This feature can be disabled by using the GUI (advanced options).
- Protocol Library—BitTorrent aggressive aging classification based on Tuple.
- Ignore filter—Filtering by VPN or VLAN is not supported.

**N/A**

In Cisco SCA BB Release 3.0.0, the limit for the number of items in the HTTP URL list was increased from 10,000 to 100,000. Adding more than 10,000 items to the list affects flow capacity. Using 100,000 list items can degrade system capacity by up to 50,000 flows compared with the capacity numbers presented in Cisco SCA BB Release 3.1.5.

**Traffic Accounting and Reporting**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to traffic accounting and reporting.

**CSCsb60539**

When you enable TUR RDRs for RTSP, the session ID field in RTSP TUR contains incorrect values because of the extraction of the session ID from the wrong fields in the RTSP packets.

**CSCsd74145**

Skype call detection is performed by using a heuristic analysis of Skype traffic, which makes call detection in Skype less accurate than in other VoIP protocols, and introduces the following limitations:

- Call start and stop event-detection can be delayed by between 30 and 60 seconds, and a single call duration measurement may involve inaccuracy of +/-30 seconds or 20 percent (the larger of the two).
- A Skype call that is carried over two connections (rather than a single connection) might not be detected.

When looking at aggregated information and reports, these limitations are of less significance, because of averaging and aggregation of large number of calls.

**N/A**

The number of concurrent sessions reported by the SCE application can sometimes be lower than the number of open flows in the SCE platform counters. In certain services, such as VoIP and FTP, a single session consists of more than one flow. The SCE platform counters track flows, rather than sessions, and therefore, may show higher values. In addition, flows with no payload are tracked by the SCE platform counters, but not by the SCE application counters.

**N/A**

The following MIB counters and fields in the Link Usage RDR and the Package Usage RDR require clarification:

- Seconds Counter—This counter is dedicated to VoIP accounting. It tracks the aggregated call duration in seconds. It is also included in Subscriber Usage RDRs.
- Seconds Counter for VoIP Services—Counts the duration of voice calls and not the duration of VoIP control flows. This makes this counter appropriate for voice usage reports; the VoIP Reports in the Reporter are based on this counter.
- Seconds Counter for Non-VoIP Services—Counts the aggregated duration of sessions.
- Concurrent Sessions Counter—Tracks the number of concurrent sessions. For voice sessions, this counter tracks the number of control sessions, not the number of calls. Inactive sessions are counted until they are terminated due to aging. Unlike the Sessions Counter, this counter shows the value at the time that the RDR is generated and not an aggregated value.
- Concurrent Active Subscribers Counter—Tracks the number of subscribers that have an open session for the reported service. For voice sessions, this counter tracks the number of subscribers that have open control sessions, rather than subscribers that have active voice calls; the number of concurrent talking subscribers cannot be deduced from this counter. Like the Concurrent Sessions Counter, this counter shows the value at the time that the RDR is generated; it is not an aggregate metric.

**Traffic Control**

This subsection describes the open caveats in SCA BB Release 3.7.1 that relate to traffic control.

**CSCsg08507**

When working in the Quota Manager with a Number of Sessions bucket and with dosage less than quota, when the dosage given to the SCE is fully used, a new session is blocked even if the quota is available in the Quota Manager. This issue occurs because there are no Quota Threshold RDRs. The (blocked) session triggers a Threshold RDR (and threshold notification to the Quota Manager) and the next session succeeds.

For example, if the dosage size is five sessions, every sixth session is blocked and fails.

**Workaround:**

Always set the dosage size equal to the quota size when working with a Number of Sessions bucket.

## Cisco SCA BB Console

This section describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to the Cisco SCA BB Console:

- [General, page 27](#)
- [Installation, page 27](#)
- [Network Navigator, page 28](#)
- [Service Configuration Editor, page 29](#)
- [Reporter, page 29](#)

### General

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to general issues concerning the SCA BB console.

#### **CSCsa91254**

Choosing Save from any tool in the SCA BB Console saves the current open PQB configuration file, even if that is not the appropriate file type for the tool.

#### **CSCsv62305**

Upgrading a device via the GUI or API also upgrades the console. If you upgrade a Protocol Pack via an SPQI file, the console is upgraded as well with the new signatures. Applying it to a device that was not upgraded as well may fail.

#### **CSCsy81384**

The Apply function fails with an error, when updating the HTTPS redirection URL as part of redirection set in the GUI.

#### **N/A**

SCA BB allows users to navigate from a report to the corresponding service configuration entity. For example, right-clicking a service name in the report legend can take you to the service definition in the Service Configuration Editor. However, the system can navigate only to the PQB file that is currently open in the SCA BB console.

#### **N/A**

Service and package names are not refreshed automatically in the Reporter after applying changes in the SCA BB Console.

#### **Workaround:**

Manually refresh the templates.

## Installation

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to installation of the Cisco SCA BB console.

### **CSCsa94964**

If you run the uninstaller when the Cisco SCA BB Console is open, the uninstallation fails without displaying any warning.

SCA BB fails to install on top of an existing installation.

### **Workaround:**

Close the Cisco SCA BB Console before starting uninstallation process.

Uninstall the SCA before reinstalling it.

### **CSCsc32003**

When the application is uninstalled, the Network Navigator configuration (sites and devices) is not deleted, instead it is kept for future Cisco SCA BB Console installations.

### **Workaround:**

To clear these settings, manually delete the C:\Documents and Settings\\.scasbb300 folder.

## Network Navigator

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to the Network Navigator.

### **CSCsa95657**

The console permits the creation of two (or more) identical devices with the same name or the same IP address.

### **Workaround:**

Remove all identical devices.

### **CSCsc49774**

Cisco SCA BB failed to connect to a device when the IP address provided is of a different device type (for example, when adding an SCE the IP address of an SM is provided). The error message displayed does not correctly identify the problem.

### **CSCsv55906**

When you upgrade Cisco SCA BB from Release 3.1.7 to Release 3.5.0, the network configuration is not automatically imported. You export, and then import. After the import is complete, two default sites appear in the window.

### **N/A**

Concurrent operations, such as applying a configuration and extracting a support file simultaneously, on the same SCE platform are not supported. Wait for one operation to finish before beginning a second operation.



**N/A**

When applying a service configuration to the SCE, the Network Navigator also updates the relevant CM with service configuration values, such as service and package names, that are later shown by the Reporter.

The Network Navigator takes the CM IP address from the SCE platform RDR-formatter definitions. With certain topologies (such as in a NAT environment), this IP address might not be accessible by the Network Navigator, and a different CM IP address should be used. The engage.ini preferences file can be used to remap CM IP addresses from the SCE platform RDR-formatter definitions to IP addresses to which the Network Navigator can connect.

The “dc.ip.remap.<n>=<address1>,<address2>” property in the engage.ini file defines a mapping between IP addresses. For example, the entry “dc.ip.remap.1=10.1.12.224,212.194.11.27” means that if the SCE RDR-formatter destination is 10.1.12.224, the Network Navigator should update the CM at 212.194.11.27.

The engage.ini file can be found and edited at the following location:

```
<scas-bb-console-installation>/plugins/policy.contribution/config
```

which usually maps to:

```
C:\Program Files\Cisco SCAS\SCAS BB
Console 3.0.0\plugins\policy.contribution_1.0.0\config\engage.ini
```

**Service Configuration Editor**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to the Service Configuration Editor.

**CSCsx17491**

PQB files that were created by using Cisco SCA BB releases earlier than Release 3.0 might not open in Cisco SCA BB Release 3.5.0 and later.

**Workaround:**

Install Cisco SCA BB 3.1.7, open the PQB and save it to the disk. You can then open it in Cisco SCA BB Release 3.5.0 and later.

**Reporter**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to the Reporter.

**CSCsy26498**

The Reporter filters the data for HTTP-related reports based on the services that belong to the HTTP protocol family. Services that are defined by flavors without a specific protocol are not included in the reports. The HTTP service based on the URL list is not displayed in the HTTP-related reports.

**Workaround:**

Add a service element for the service that includes flavor and HTTP protocol.

**CSCta54572**

All the reports that show average bandwidth per subscriber are not accurate.

The three reports that show the average bandwidth per subscriber are:

- Average Subscriber Bandwidth
- Average Subscriber Bandwidth Per Service
- Tunneled IPv6 Average Subscriber Bandwidth

These reports sum up the number of subscribers from all RDRs per hour instead of the average number of subscribers per hour, and divide the total bandwidth with this number.

For example:

If RDR is per minute and there are 1000 active subscribers, the report divides the total bandwidth in 60,000 (1000 \* 60 minutes).

**CSCtc31584**

Average or global subscriber bandwidth reports should not allow filter by service.

The reports for Average Subscriber Bandwidth and Tunneled IPv6 Average Subscriber Bandwidth with filter by services using the right pane generate inaccurate results.

**Workaround:**

When generating reports for Average subscriber bandwidth and Tunneled IPv6 Average Subscriber Bandwidth, do not filter by services using the right pane.

**CSCtc31659**

The IPv6 vs IPv4 Bandwidth Comparison report is incorrect when using aggregation.

This report is the result of the union between two queries operated on RPT\_LUR and RPT\_GUR simultaneously.

Data must be merged but only the RPT\_LUR table supports aggregations, so the report produces incorrect results.

**Workaround:**

Disable the aggregation for the RPT\_LUR table.

## Configuration Management

This section describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to configuration management.

### Service Configuration API

This subsection describes the open caveats in Cisco SCA BB Release 3.7.1 that relate to the Service Configuration API.

#### N/A

Backward compatibility with SCA BB 2.5 Service Configuration API.

Package and class name changes: The Service Configuration Management API has changed in Cisco SCA BB Release 3.0.0, to accommodate new product naming conventions. Nevertheless, the older API classes and methods can still be used.



#### Note

---

However, the Service Configuration Editing API in Cisco SCA BB 3.0.0 has been significantly changed, and is generally incompatible with Cisco SCA BB Release 2.5.0.

---

CSV file format changes: SCA BB introduces a new format for CSV files of HTTP URL lists. For backward compatibility, SCA BB 3.0.0 Service Configuration API allows importing CSV files of HTTP URLs in the old Cisco SCA BB Release 2.5.0. formats.

# Cisco Service Control Application for Broadband Release 3.7.0

This section describes the new features, and resolved and open issues pertaining to Cisco SCA BB Release 3.7.0:

- [New Features, page 20](#)
- [Protocol Support, page 20](#)
- [Resolved Caveats, Release 3.7.0, page 20](#)
- [Open Caveats, Release 3.7.0, page 22](#)

## New Features

The Cisco SCA BB Release 3.7.0 introduces the following features:

- Advanced SMTP detection
- Updated antispam and antiharvest features
- Anti spam protocol compliancy
- Block TCP Port 25 on spam detection
- Anonymous group manager GUI tool
- NAT gateway detection using OS fingerprinting
- New fields in Transaction Usage RDRs
- Anonymized RDRs

See *Cisco Service Control Application for Broadband User Guide* for a complete description of these features.

## Protocol Support

See the Protocol Pack Notes for information about protocol support for Protocol Pack #24 (included in Cisco SCA BB 3.7.0).

**Note**

---

When you upgrade old PQB files, new signature-based protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as *Default Service*. To resolve this issue, manually assign these protocols to a service.

---

## Resolved Caveats, Release 3.7.0

This section describes the caveats resolved in Cisco SCA BB Release 3.7.0:

- [SCA BB Console, page 21](#)
- [Reporter, page 21](#)
- [Subscriber Manager GUI, page 22](#)

## SCA BB Console

This subsection describes resolved caveats in Cisco SCA BB Release 3.7.0 that relate to the general issues concerning the Cisco SCA BB Console.

### **CSCtk94737**

WinnyP was not configurable from Cisco SCA BB Console.

This issue is resolved. You can now enable WinnyP from Cisco SCA BB Console.

### **CSCtl03931**

The Global Controller unit conversion was not accurate.

In Cisco SCA BB Console, under Global Controller Settings, the unit for the rate limit was displayed in KB/s. The value displayed in the Global Policy screen, was converted to KB/s by dividing the MB/s value by 1000 rather than by 1024.

This issue is resolved.

### **CSCtl19613**

Failed to anonymize IP address for RDRs other than HTTP.

This issue is resolved. A new check box is introduced to enable and disable anonymization in other RDRs such as Blocking RDR, Spam RDR, and Flow Start RDR.

### **CSCtn65110**

The Subscriber Manager GUI failed to open from Cisco SCA BB console when a Collection Manager IP address was configured in the p3sm.cfg file.

This issue is resolved.

### **CSCtq12506**

An error was displayed when trying to load a PQB file or retrieve a PQB file from the SCE in Cisco SCA BB Console.

```
An internal error occurred during: "Opening Service Configuration File".
org.eclipse.emf.ecore.resource.Resource$IOWrappedException: The entity name must
immediately follow the '&' in the entity reference.
```

This error was caused because the name of a Zone contained the “&” character.

This issue is resolved. You cannot include the “&” character in the Flavor and Zone names.

## Reporter

This subsection describes the resolved caveats in Cisco SCA Reporter Release 3.7.0.

### **CSCtn64715**

Large number of malicious sessions were seen on SCA Reporter.

When a report was generated after the SCE detected an attack (Port Scan), reports for Top Scanning or Attacking host showed a large number of malicious sessions.

This issue is resolved.

## Subscriber Manager GUI

This section describes resolved caveats in Cisco SCA BB Subscriber Manager GUI:

### CSCsw79014 and CSCtd16202

These issues with the Subscriber Manager Client GUI make it practically unusable:

- CSCsr09226—In Release 3.5.0 Subscriber Manager GUI, while using VLAN SM GUI, Cisco SCA BB failed to change the subscriber name and the subscriber was removed.
- CSCsj45511—In Release 3.1.5LA GUI, window froze and was unable to work with the Subscriber Manager.
- CSCsh57287—Subscriber Manager GUI was not up-to-date with Subscriber Manager database.
- CSCso30235—Exporting subscribers failed with Subscriber Manager GUI release 3.1.5 and 3.1.0.
- CSCsi03280—Subscriber Manager GUI could be connected to an SCE.
- CSCsh96714—A logic problem occurred while changing the subscriber domain.
- CSCsh57286GUI—An SM GUI error appeared while searching for a subscriber and the database was empty
- CSCsl48003—A faulty radio button operation added VLAN and IP for each subscriber.
- CSCsl16383—There was a limit to the number of characters when a subscriber was added to the SM GUI.
- CSCsl47880—You cannot add a subscriber with more than 40 characters.
- CSCsw18320—Subscriber details were not refreshed automatically.

## Open Caveats, Release 3.7.0

This section describes the open caveats in Cisco SCA BB Release 3.7.0:

- [Traffic Processing, page 22](#)
- [Cisco SCA BB Console, page 26](#)
- [Configuration Management, page 31](#)

## Traffic Processing

This section describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to traffic processing:

- [General, page 22](#)
- [Traffic Classification, page 24](#)
- [Traffic Accounting and Reporting, page 25](#)
- [Traffic Control, page 26](#)

### General

This section describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to general issues concerning traffic processing.

**CSCtq12796**

In the Anonymous Group Manager GUI tool, the values for Template ID, Package ID, UpVlink, and DownVlink are restricted to 99. But in SCE, the values for Template ID and Package ID are restricted to 4999, and values for UpVlink, DownVlink are restricted to 1023. The values supported should be same in both the GUI and the SCE.

**Workaround:**

No known workaround.

**CSCtq12777**

Failed to connect to multiple Subscriber Managers by using the Subscriber Manager GUI in Cisco SCA BB Console.

When connected to a Subscriber Manager, if you try to connect to a second Subscriber Manager, the first Subscriber Manager gets replaced with the second Subscriber Manager.

**Workaround:**

No known workaround.

**CSCtq15400**

If two zeroes are added to a new Protocol ID to avoid ID duplication, the issue gets resolved only after two attempts. Also, even if you use a new ID in the second attempt, the ID you entered during the first attempt is saved.

For example, if the new Protocol ID is 4200, the first attempt fails. In the second attempt, even if you use a new ID (4211), 4200 is saved as the new Protocol ID.

**Workaround:**

If you use two zeroes, enter the same value during both the attempts.

**CSCsx75003**

The PQI installation process should reserve more disk space on SCE 2000.

The PQI installation process fails because of insufficient disk space on the SCE 2000. The SCE file system containing a lot of files consumes the disk space.

**Workaround:**

Manually remove the unnecessary files from the SCE file system.

**CSCsz59158**

The SCE 8000 MGBE might crash when you apply a PQB that contains 1000 global controllers.

If a policy with 1000 global controllers is not applied correctly after a reload, the SCE might run out of memory and the box may crash.

**Workaround:**

There is no known workaround.

**CSCtq99331**

When applying policies for different templates, if the virtual link is enabled, an error similar to this appears:

```
+ 6/16/11 5:41:17 PM IST | ERROR | Failed to apply service configuration at "SCE device
[10.78.241.106]": Error Code = 1, Description: "Input key should be number between 0 to
4,294,967,295More info: in func 'CmdLut::overwriteManyCfg',
lutName='GT_LUT_VIRTUAL_upLinkId2AppAGCIdx', key[0]='-65536', value[0]='0',
numVariables=3..", Detailed: "" (LUT_overwriteManyCfg:{key=[Ljava.lang.String;@21f572,
slot=0, lutName=GT_LUT_VIRTUAL_upLinkId2AppAGCIdx, value=[Ljava.lang.String;@21f579})
```

**Workaround:**

Disable the virtual link in SCE using the **no virtual link** CLU command before applying the new configuration.

**Traffic Classification**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to traffic classification.

**CSCsd81077**

The same flow can be classified into different services, depending on a zone configuration that seems unrelated. This occurs after you define a new port-based protocol and then create a new service, adding a service element with the new protocol and a non-default zone to the service. Flows that match the new protocol but do not match the zone of the service element are now mapped to the Default Service.

Complete these steps (The unexpected flow classification occurs at step 6):

1. Add a new port-based protocol. For example, doom2 on TCP port 6666. Do not add the protocol to any service.
2. The SCE now classifies flows that match the doom2 protocol (TCP on port 6666) as Generic TCP, as expected.
3. Add a zone named gaming servers.
4. Create a new service called doom2 gaming servers. Add a service element, where the Protocol is doom2 and the Zone is gaming servers.
5. The SCE now classifies flows that match the doom2 protocol and the gaming servers zone to the new doom2 gaming servers service, as expected.
6. However, flows that match the doom2 protocols, but *do not* match the gaming servers zone, is classified as Default Service instead of Generic TCP.
7. If you delete the doom2 gaming servers service, the same flows that were classified as Default Service, is again classified (correctly) as Generic TCP.

**Workaround:**

Add the service element <New port-based protocol, Initiated by either side, \*, \*> to an existing service. (You can also define a new service for this purpose.) After you do that, transactions using the specific protocol but with network IP addresses that do not match the specific zone, go to the less specific service.

For the example given above, add the service element <doom2, Initiated by either side, \*, \*> to the Generic TCP service.



**CSCsi46655**

When SCA BB is deployed in an environment where it is required to analyze traffic in VLANs/VPNs with overlapping IP addresses, some of its capabilities, which rely on uniqueness of IP addresses in the network, do not function:

- Classification—No support for zones.
- Reporting—Reports based on IP addresses in Transaction RDRs are not accurate.

Many reports in the following categories rely on IP uniqueness:

- Mail and News
- Traffic Discovery—Statistics
- Web and Streaming
- Protocol Library—Mechanism based on IP addresses. This feature can be disabled by using the GUI (advanced options).
- Protocol Library—BitTorrent aggressive aging classification based on Tuple.
- Ignore filter—Filtering by VPN or VLAN is not supported.

**N/A**

In Cisco SCA BB Release 3.0.0, the limit for the number of items in the HTTP URL list was increased from 10,000 to 100,000. Adding more than 10,000 items to the list affects flow capacity. Using 100,000 list items can degrade system capacity by up to 50,000 flows compared with the capacity numbers presented in Cisco SCA BB Release 3.1.5.

**Traffic Accounting and Reporting**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to traffic accounting and reporting.

**CSCsb60539**

When you enable TUR RDRs for RTSP, the session ID field in RTSP TUR contains incorrect values because of the extraction of the session ID from the wrong fields in the RTSP packets.

**CSCsd74145**

Skype call detection is performed by using a heuristic analysis of Skype traffic, which makes call detection in Skype less accurate than in other VoIP protocols, and introduces the following limitations:

- Call start and stop event-detection can be delayed by between 30 and 60 seconds, and a single call duration measurement may involve inaccuracy of +/-30 seconds or 20 percent (the larger of the two).
- A Skype call that is carried over two connections (rather than a single connection) might not be detected.

When looking at aggregated information and reports, these limitations are of less significance, because of averaging and aggregation of large number of calls.

**N/A**

The number of concurrent sessions reported by the SCE application can sometimes be lower than the number of open flows in the SCE platform counters. In certain services, such as VoIP and FTP, a single session consists of more than one flow. The SCE platform counters track flows, rather than sessions, and therefore, may show higher values. In addition, flows with no payload are tracked by the SCE platform counters, but not by the SCE application counters.

**N/A**

The following MIB counters and fields in the Link Usage RDR and the Package Usage RDR require clarification:

- **Seconds Counter**—This counter is dedicated to VoIP accounting. It tracks the aggregated call duration in seconds. It is also included in Subscriber Usage RDRs.
- **Seconds Counter for VoIP Services**—Counts the duration of voice calls and not the duration of VoIP control flows. This makes this counter appropriate for voice usage reports; the VoIP Reports in the Reporter are based on this counter.
- **Seconds Counter for Non-VoIP Services**—Counts the aggregated duration of sessions.
- **Concurrent Sessions Counter**—Tracks the number of concurrent sessions. For voice sessions, this counter tracks the number of control sessions, not the number of calls. Inactive sessions are counted until they are terminated due to aging. Unlike the Sessions Counter, this counter shows the value at the time that the RDR is generated and not an aggregated value.
- **Concurrent Active Subscribers Counter**—Tracks the number of subscribers that have an open session for the reported service. For voice sessions, this counter tracks the number of subscribers that have open control sessions, rather than subscribers that have active voice calls; the number of concurrent talking subscribers cannot be deduced from this counter. Like the Concurrent Sessions Counter, this counter shows the value at the time that the RDR is generated; it is not an aggregate metric.

**Traffic Control**

This subsection describes the open caveats in SCA BB Release 3.7.0 that relate to traffic control.

**CSCsg08507**

When working in the Quota Manager with a Number of Sessions bucket and with dosage less than quota, when the dosage given to the SCE is fully used, a new session is blocked even if the quota is available in the Quota Manager. This issue occurs because there are no Quota Threshold RDRs. The (blocked) session triggers a Threshold RDR (and threshold notification to the Quota Manager) and the next session succeeds.

For example, if the dosage size is five sessions, every sixth session is blocked and fails.

**Workaround:**

Always set the dosage size equal to the quota size when working with a Number of Sessions bucket.

**Cisco SCA BB Console**

This section describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to the Cisco SCA BB Console:

- [General, page 27](#)
- [Installation, page 27](#)
- [Network Navigator, page 28](#)
- [Service Configuration Editor, page 29](#)
- [Reporter, page 29](#)

## General

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to general issues concerning the SCA BB console.

### **CSCsa91254**

Choosing Save from any tool in the SCA BB Console saves the current open PQB configuration file, even if that is not the appropriate file type for the tool.

### **CSCsv62305**

Upgrading a device via the GUI or API also upgrades the console. If you upgrade a Protocol Pack via an SPQI file, the console is upgraded as well with the new signatures. Applying it to a device that was not upgraded as well may fail.

### **CSCsy81384**

The Apply function fails with an error, when updating the HTTPS redirection URL as part of redirection set in the GUI.

### **N/A**

SCA BB allows users to navigate from a report to the corresponding service configuration entity. For example, right-clicking a service name in the report legend can take you to the service definition in the Service Configuration Editor. However, the system can navigate only to the PQB file that is currently open in the SCA BB console.

### **N/A**

Service and package names are not refreshed automatically in the Reporter after applying changes in the SCA BB Console.

### **Workaround:**

Manually refresh the templates.

## Installation

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to installation of the Cisco SCA BB console.

### **CSCsa94964**

If you run the uninstaller when the Cisco SCA BB Console is open, the uninstallation fails without displaying any warning.

SCA BB fails to install on top of an existing installation.

### **Workaround:**

Close the Cisco SCA BB Console before starting uninstallation process.

Uninstall the SCA before reinstalling it.

**CSCsc32003**

When the application is uninstalled, the Network Navigator configuration (sites and devices) is not deleted, instead it is kept for future Cisco SCA BB Console installations. \

**Workaround:**

To clear these settings, manually delete the C:\Documents and Settings\\.scasbb300 folder.

**Network Navigator**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to the Network Navigator.

**CSCsa95657**

The console permits the creation of two (or more) identical devices with the same name or the same IP address.

**Workaround:**

Remove all identical devices.

**CSCsc49774**

Cisco SCA BB failed to connect to a device when the IP address provided is of a different device type (for example, when adding an SCE the IP address of an SM is provided). The error message displayed does not correctly identify the problem.

**CSCsv55906**

When you upgrade Cisco SCA BB from Release 3.1.7 to Release 3.5.0, the network configuration is not automatically imported. You export, and then import. After the import is complete, two default sites appear in the window.

**N/A**

Concurrent operations, such as applying a configuration and extracting a support file simultaneously, on the same SCE platform are not supported. Wait for one operation to finish before beginning a second operation.

**N/A**

When applying a service configuration to the SCE, the Network Navigator also updates the relevant CM with service configuration values, such as service and package names, that are later shown by the Reporter.

The Network Navigator takes the CM IP address from the SCE platform RDR-formatter definitions. With certain topologies (such as in a NAT environment), this IP address might not be accessible by the Network Navigator, and a different CM IP address should be used. The engage.ini preferences file can be used to remap CM IP addresses from the SCE platform RDR-formatter definitions to IP addresses to which the Network Navigator can connect.

The “dc.ip.remap.<n>=<address1>,<address2>” property in the engage.ini file defines a mapping between IP addresses. For example, the entry “dc.ip.remap.1=10.1.12.224,212.194.11.27” means that if the SCE RDR-formatter destination is 10.1.12.224, the Network Navigator should update the CM at 212.194.11.27.

The engage.ini file can be found and edited at the following location:

```
<scas-bb-console-installation>/plugins/policy.contribution/config
```

which usually maps to:

```
C:\Program Files\Cisco SCAS\SCAS BB
Console 3.0.0\plugins\policy.contribution_1.0.0\config\engage.ini
```

**Service Configuration Editor**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to the Service Configuration Editor.

**CSCsx17491**

PQB files that were created by using Cisco SCA BB releases earlier than Release 3.0 might not open in Cisco SCA BB Release 3.5.0 and later.

**Workaround:**

Install Cisco SCA BB 3.1.7, open the PQB and save it to the disk. You can then open it in Cisco SCA BB Release 3.5.0 and later.

**Reporter**

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to the Reporter.

**CSCsy26498**

The Reporter filters the data for HTTP-related reports based on the services that belong to the HTTP protocol family. Services that are defined by flavors without a specific protocol are not included in the reports. The HTTP service based on the URL list is not displayed in the HTTP-related reports.

**Workaround:**

Add a service element for the service that includes flavor and HTTP protocol.

**CSCta54572**

All the reports that show average bandwidth per subscriber are not accurate.

The three reports that show the average bandwidth per subscriber are:

- Average Subscriber Bandwidth
- Average Subscriber Bandwidth Per Service
- Tunneled IPv6 Average Subscriber Bandwidth

These reports sum up the number of subscribers from all RDRs per hour instead of the average number of subscribers per hour, and divide the total bandwidth with this number.

For example:

If RDR is per minute and there are 1000 active subscribers, the report divides the total bandwidth in 60,000 (1000 \* 60 minutes).

**CSCtc31584**

Average or global subscriber bandwidth reports should not allow filter by service.

The reports for Average Subscriber Bandwidth and Tunneled IPv6 Average Subscriber Bandwidth with filter by services using the right pane generate inaccurate results.

**Workaround:**

When generating reports for Average subscriber bandwidth and Tunneled IPv6 Average Subscriber Bandwidth, do not filter by services using the right pane.

**CSCtc31659**

The IPv6 vs IPv4 Bandwidth Comparison report is incorrect when using aggregation.

This report is the result of the union between two queries operated on RPT\_LUR and RPT\_GUR simultaneously.

Data must be merged but only the RPT\_LUR table supports aggregations, so the report produces incorrect results.

**Workaround:**

Disable the aggregation for the RPT\_LUR table.

## Configuration Management

This section describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to configuration management.

### Service Configuration API

This subsection describes the open caveats in Cisco SCA BB Release 3.7.0 that relate to the Service Configuration API.

#### N/A

Backward compatibility with SCA BB 2.5 Service Configuration API.

Package and class name changes: The Service Configuration Management API has changed in Cisco SCA BB Release 3.0.0, to accommodate new product naming conventions. Nevertheless, the older API classes and methods can still be used.



#### Note

However, the Service Configuration Editing API in Cisco SCA BB 3.0.0 has been significantly changed, and is generally incompatible with Cisco SCA BB Release 2.5.0.

CSV file format changes: SCA BB introduces a new format for CSV files of HTTP URL lists. For backward compatibility, SCA BB 3.0.0 Service Configuration API allows importing CSV files of HTTP URLs in the old Cisco SCA BB Release 2.5.0. formats.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Overview" section.

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](http://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 and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2010-2012 Cisco Systems, Inc. All rights reserved.

