Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.5.0

Revised: April 13. 2011, OL-14439-09

These release notes for Cisco SCA BB describe the enhancements provided in Cisco SCA BB Release 3.5.0. These release notes are updated as needed.

For a list of the caveats that apply to Cisco SCA BB Release 3.5.0, see Open Caveats, page 9.

For information regarding features added and issues resolved in the 3.1.x train, please refer to:

- Release Notes for Cisco Service Control Application for Broadband (SCA BB) 3.1.7

For further information about related products, please refer to 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 Download Guide containing the compatibility matrix, refer to the following:

Cisco Service Control Application for Broadband Download Guide

Contents

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

Introduction

This document describes the new functionality, enhancements, and known issues in SCA BB release 3.5.0.

It is assumed that the reader already has a good working knowledge of the Cisco Service Control solution. For additional information, please refer to the Cisco SCA BB documentation.

Note Cisco has been streamlining and improving its user interface. To access the new Cisco Service Control online documentation site, please do the following:

1. Go to the following page on Cisco.com: http://www.cisco.com/web/psa/products/index.html.
2. From the **Select a category** list, select 'Service Exchange'.
3. From the **Select a sub-category** list, select the desired Cisco Service Control category.
4. From the **Select a product** list, select the desired Cisco Service Control product.

Note Operation of the SCA BB GUI Console is not supported on VMWare.

SCA BB Release 3.5.0

This section describes the resolved issues of SCA BB release 3.5.0.

Information About New Features

The following section lists the major new features in SCA BB 3.5.0. See the *Cisco Service Control Application for Broadband User Guide* for a complete description of these features.

Behavioral Targeting

The SCE now includes a solution for behavioral targeted advertising that allows Service Providers to participate in the advertising value chain. This solution enables Service Providers to increase ARPU through a revenue sharing model while addressing privacy concerns through advanced Opt-in / Opt-out mechanisms.

The solution is comprised of several tools that allow integration with multiple advertising partners:

- Traffic mirroring - sending a copy of selected HTTP traffic to a 3rd party server, using VLAN marking. This capability is used in behavioral targeting and may also be used for other solutions such as, LI / CALEA, Video caching, and identifying and mitigating copyright infringing P2P downloads.
- Reporting HTTP ClickStream information in RDR records and making the subscriber details anonymous in these records. ClickStream is the ability to associate HTTP requests with a subscribers ClickStream, and enables gathering information about a subscribers browsing habits. ClickStream events constitute only 1%-5% of the total amount of HTTP requests, which reduces the amount of data to be analyzed.

- Enhanced HTTP redirect - additional parameters can be added to the redirected message for inserting in WiFi.

  The Redirect operation is enhanced with the following configuration options:

  - Redirect once
  - Redirect always
  - Redirect periodically
    - Only every T seconds
    - Only once, every V Kbytes
    - Only once, every X clicking events
  - Redirect until the subscriber browses to a dismissal URL

  New fields in the HTTP Redirect packet for advanced use cases of smarter redirection by the redirect server. You can to choose whether to include each of the following fields:

  - Service ID
  - Subscriber ID
  - Timestamp
  - String (configurable by the user)
  - Referrer
  - Distinct ID, which is composed of an incremental-number or an SCE traffic processor number
  - Cookie
  - Original host
  - Original URL
  - Original parameters

  The Redirect operation now includes the option to select an HTTP code value (like 302 or 304) and string

Congestion Control Through CMTS Awareness

Congestion Control through CMTS awareness allows automatically tying DPI bandwidth management into CMTS physical interfaces so subscribers or applications can be de-prioritized in reaction to HFC bandwidth congestion. The solution is application and subscriber aware - different actions can be applied to different applications and subscribers. The solution is also topology aware and includes automatic real time tracking of each of the CMTS upstream and downstream interfaces. Congestion at the CMTS RF interfaces can be avoided through measuring bandwidth per upstream / downstream prioritizing only when required CMTS awareness is implemented in a MSOs network through the SCE integrating with CMTS's for automatically identifying existing RF interfaces and their associated speeds. The SCE keeps traffic within an upstream / downstream below the physical limit through mapping interface traffic into a virtual pipe (implemented based on SCE Global Controllers).

The SCE performs preferential bandwidth control - based on application tiers keeping the interface's utilization below a certain threshold for bounding the delay on that interface.

Mitigating Outgoing SPAM

The outgoing SPAM mitigation solution is enhanced with the ability to set the identification and mitigation per package. The following parameters can now be configured per package:

- SPAM identification thresholds
- Sending an RDR
- Subscriber notification
- Blocking

Increased Number Of Concurrent Subscribers

The number of concurrent subscribers on the SCE2020 and SCE8000 is increased as follows:

- SCE2020: In previous releases, there are 80K, and in release 3.5.0, there are 200K concurrent subscribers.
- SCE8000: In previous releases, there are 250K, and in release 3.5.0, there are 1M concurrent subscribers.

The number of supported concurrent subscribers is set to several discrete options. Each discrete option influences the amount of supported flows.

Enhancing The SCA BB Reporter

In release 3.5.0, the SCA BB Reporter is enhanced with the following new features:

- Favorite Reports - A favorites section is added to the reporter. All favorite/common reports can be executed from this tab.
- Reports Hierarchy - This new functionality allows focusing on the most active services and on a specific category of services. You can define the level of hierarchy presented, adapting the report interactively.
- Printing, e-mailing, and exporting reports to PDF format.
- New report templates: Infected subscribers vs. active subscribers, Average bandwidth per subscriber over all services, Average bandwidth per subscriber for a single service, Total active subscribers and other new report templates.

SCE8000 Enhancements

Release 3.5.0 includes multiple enhancements for the SCE8000:

- Increased performance per blade to up to 15Gbps. 15Gbps refers to the BW of the link before the SCE is added.
- SCE8000 active-standby fail over through Cascade support on the SCE8000.
- SNTP (Simple Network Timing Protocol) on the SCE8000.
- IPinIP on the SCE8000.
- SCE8000 Device monitoring.
  - CLI command for showing the temperature within the device
  - Detailed User Log indications for system failure events - Power Supply, FAN, etc.

  - CLI command for status of the PSU and FANs

Classification Enhancements

The SCE's classification capabilities are enhanced in release 3.5.0:

- Instant Messaging and SMTP - IM traffic separation - Separating VoIP over IM from Chat and File-Transfer.
- Distinguishing between Authenticated and non-authenticated SMTP (AUTH command).
- Multi-Transaction Classification for HTTP - The SCE can now classify all 'GET' requests over a single http TCP flow. This allows more secured and accurate support for flavors and blacklists. Each request / response is treated as a stand-alone transaction so reporting / control can be separately applied.
- Multi-Stage Classification - today the SCE's classification process may last for up to several tens or even hundreds of packets mainly due to the need to classify encrypted protocols. This new feature allows generating a first-stage, quick, temporary classification result for allowing you to enforce more restricted policies. As the SCE processes more of the flow's packets the initial classification decision may change. At every classification stage, an updated classification to Protocol Type is provided and the mapping to Service may be adjusted.

UI and Operational Enhancements

The user interface and operational concepts are enhanced in release 3.5.0:

- Streamlined upgrade - Parallel upgrade of multiple SCEs
- Parallel apply action of policy on multiple SCEs - up to 5 SCEs in parallel
- Updated Traffic Tree:
  - Addressing new trends in Internet and Video protocols and applications
  - New structure with better partitioning of protocols
  - Reflects a more consistent classification taxonomy and terminology
  - New and advanced tool for navigation in the traffic tree that allows searching for Service, Protocol, port numbers, etc.
- More Intuitive BW-control Configuration and representation:
  - Global Policy View
  - Wizard for adding a new GC and mapping BWCs and rules to it
  - GCs and their rules can be filtered and viewed without the BWCs
  - The GC and total BW are configured in absolute values and not in percentages

Flow Capture

Flow capturing functionality is added on the SCE for capturing subscriber traffic for multiple troubleshooting use cases. Layer 3 attributes like address ranges define the traffic to capture.

The captured traffic is accumulated in a .cap file and stored in a remote FTP destination.

Subscriber Manager and Collection Manager Enhancements

- Subscriber Manager
  - Support for Java 1.5
  - Support for Veritas Cluster Server 5
  - SM and SCE pre-loaded with LEGs
- Collection Manager
  - Easy to use upgrade procedure
  - Provides information on RDR rate per table
  - Maintenance scripts for MySQL & Oracle
  - Support for Java 1.5 and RHL5
  - Support for external databases: MySQL 5.1, Oracle 11

Protected URL Database

The SCE Protected URL Database is a database that contains a "blacklist," a list of websites that are considered off limits or dangerous. The SCE can be configured to apply a specific action, such as blocking a site, when a subscriber attempts to access a site listed on the blacklist.

The database is encrypted so that no one, including the operator, can view the blacklist. The blacklist is managed on the SCE and cannot be withdrawn to the management PC.

RDRs are created when a subscriber attempts to access a link included in the blacklist. However, the RDRs do not contains the URL or Host information of the site.

Protocol Support

Refer to the Protocol Pack Notes for information regarding protocol support for Protocol Pack #15 (included in SCA BB 3.5.0).

Note When upgrading 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 fix this, manually assign these protocols to a service.

Resolved Caveats

This section describes caveats that are resolved in SCA BB release 3.5.0.

CSCsd52274

GC value does not change if the management agent is down during the time frame change

When the management agent is down (during a boot or PQI installation), if the time frame changes, the GC value does not consistently change to the value of the new time frame once the management agent is back up.

This issue is resolved in release 3.5.0.

CSCsg14757

Port congestion may cause inconsistent behavior

When there are many subscribers, and low GC values, high congestion factors are required in order to converge. Therefore, the subscribers connected to the low GC are starved with no fair reason from the user's perspective (business and policy wise).

This issue is resolved in release 3.5.0.

CSCsg29991

Changing the port of the PRPC server cause failure

If the PRPC server port in a device (SM/CM/SCE) is changed, many GUI actions create the PRPC connection in the same way that retrieves the correct PRPC port from the configuration file, while apply retrieves the session object in a different way.

This issue is resolved in release 3.5.0.

CSCsg45603

SM GUI - Remove mapping does not logout the subscriber

From the GUI, you add a subscriber. The subscriber appears in the GUI and in the SM. After removing the subscriber IP mapping from the GUI, the subscriber IP mapping remains in the SM and in the Edit Subscriber window.

This issue is resolved in release 3.5.0.

CSCsi86983

Virtual links is not supported for the SCE1010 platform

Applying a service configuration fails on SCE1010 when virtual links mode is switched on. Hence, virtual links is not supported for SCE1010 platforms.

This issue is resolved in release 3.5.0.

CSCsl52081

Multi-threading support is lacking when using Service Configuration API

When applying the customer's service configuration into the SCEs by a multi-threaded API program, API errors are returned from multiple SCEs.

This issue is resolved in release 3.5.0.

CSCsl74259

DURATION field in Usage RDRs should show actual duration

The DURATION field in Usage RDRs contains the configured duration rather than the actual duration.

This issue is resolved in release 3.5.0.

CSCsm37063

Problem applying pre-3.1.5 service configurations to SCA BB 3.1.5 and higher

There is a problem applying some service configuration/PP combinations (3.0.6PP#10, 3.1.0PP#10, 3.1.0PP#12) to SCA BB 3.1.5 installed with PP#12 and higher or 3.1.6 PP#13 and higher.

For example:

1. Install 315 PQI.

2. Open 310PP#12-pqb-service configuration in the SCA BB 3.1.5 Console.
3. Apply the service configuration to 3.1.5 SCE FCS.
4. Try to install SPQI 315PP#12.

The following error is displayed:

```
1/24/08 3:00:21 PM IST | ERROR | Protocol Pack Installation on 'SCE 315' [192.118.77.20]:
Operation failed: Error while importing DSS: Item uniqueness violation error: duplicate
Protocol Element
```

This issue is resolved in release 3.5.0.

CSCsm57690

Apply operation tries to update CM address 127.0.0.1

When applying a PQB, the following error messages is generated: "Failed to update CM at 127.0.0.1 with service configuration values: Connection refused: connect". This happens only when a local RDR-server is configured: RDR-formatter destination 127.0.0.1 port 33001 category number 4 priority 100.

This issue is resolved in release 3.5.0.

CSCso85051

Separation of interval configuration of Accounting (ISG) RDR's from NURs

For the Accounting RDR, the reporting is controlled by the following advance setting options:

- Flow Accounting RDRs enabled
- Flow Accounting RDRs limit per seconds - specifies max RDR rate
- Flow Accounting RDRs interval for each service (in seconds) - specifies interval between RDRs

This issue is resolved in release 3.5.0.

CSCsq72143

SCE8000 limits minimum GC to 1.6M

SCE8000 limits the minimum GC to 1.6M, although the GC can be configured to 16K via the CLI.

This issue is resolved in release 3.5.0.

CSCsq73623

sce-url-db should not be cleared silently

When you perform some sce-url-db operations related to protection, the SCE clears the URL database silently without notifying the user.

This issue is resolved in release 3.5.0.

CSCsr50955

SCE external URL filtering fails if URL path contains "%"

The SCE external URL filtering might incorrectly classify URLs that contain "%" in the path part of the URL.

This issue is resolved in release 3.5.0.

CSCsv78126

Default TR rate limit of 250 RDRS per sec is way too high

The current default policy sets the Transaction RDRs rate limit to a value of 250 RDRs per second. This value is too high and should be set no higher than 100 as it was in 3.1.X

This issue is resolved in release 3.5.0.

Open Caveats

Traffic Processing

This section describes open caveats in SCA BB release 3.5.0 that relate to traffic processing.

Traffic Classification

This subsection describes open caveats in SCA BB release 3.5.0 that relate to traffic classification.

CSCsd81077

Unexpected flow classification after adding service element with non-default zone

The same flow can be classified to 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 will now be mapped to the Default Service.

The following steps illustrate this. 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 will now classify 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 “doom2 gaming servers”. Add a service-element where protocol=“doom2” and zone=“gaming servers”.
5. The SCE will now classify 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, will be 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”, will again be 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.) Once you do that, transactions using the specific protocol but with network IP addresses that do not match the specific zone, will 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

Limitations when working with VLANS/VPNs with overlapping IPs

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 - lately used mechanism based on IP addresses. This feature can be disabled 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

Flow capacity deteriorates when HTTP URL table is full

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

Traffic Accounting and Reporting

This subsection describes open caveats in SCA BB release 3.5.0 that relate to traffic accounting and reporting.

CSCsb60539

Incorrect Values in Session ID field in RTSP TUR

When enabling TUR RDRs for RTSP, the session ID field in RTSP TUR contains incorrect values due to the session ID being extracted from the wrong place in the RTSP packets.

CSCsd74145

Skype reporting limitations

Skype call detection is done 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% (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, due to averaging and aggregation of large number of calls.

N/A

Concurrent sessions reported by SCE application lower than open flows reported by SCE platform

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 is made 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

Clarification regarding VoIP accounting

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 open caveats in SCA BB release 3.5.0 that relate to traffic control.

CSCsg08507

Quota Threshold RDRs are not supported for Number of Sessions bucket

When working in the QM 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 will be blocked even if there is still quota in the QM, since there are no Quota Threshold RDRs. This (blocked) session will trigger a Threshold RDR (and threshold notification to the QM); therefore the next session will succeed.

For example, if the dosage size is 5 sessions, every 6th session will be blocked and will fail.

Workaround:

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

CSCsy73995

BWC with unlimited PIR limits subscriber traffic to 500 mbps

A subscriber Bandwidth Controller (BWC) with unlimited PIR that is connected to an unlimited Global Controller actually limits the subscriber bandwidth to 500 mbps instead of allowing unlimited rate.

Therefore, if a subscriber transmits more than 500 mbps of traffic, the SCE platform will limit the traffic to 500 mbps, even if the BWC is set to Unlimited

Workaround:

None

SCA BB Console

This section describes open caveats in SCA BB release 3.5.0 that relate to the SCA BB console.

General

This subsection describes open caveats in SCA BB release 3.5.0 that relate to general issues concerning the SCA BB console.

CSCsa91254

A PQB file is saved when Save is selected from tools other than the Service Configuration Editor

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

CSCsu88253

Welcome page does not always open from some views

Depending on the open view, the Welcome page does not appear or appears in a different location within the SCA BB console.

CSCsv62305

GUI cannot apply to all SCA BB versions

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.

CSCsw51179

Applying a policy to an SCE with a lower PP version

You can apply a policy with a GUI that is upgraded to a higher PP version than the SCE it is applying the policy to. This can cause new signatures that seem to be controlled by the SCE to actually not be handled since the SCE is not aware of them.

CSCsw63256

Installing a SPQI via the GUI is required to be able to apply a policy to SCEs

When you perform a protocol pack upgrade via the GUI or the servconf application, a special module is extracted to **C:\Documents and Settings\user\.p-cube**. If this module does not exist an apply to the relevant SCEs might fail.

N/A

Limitations in navigating from the Reporter to the Service Configuration Editor

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's 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

After applying a service configuration, service and package names are not refreshed in the Reporter

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

Workaround:

Refresh the templates manually.

Installation

This subsection describes open caveats in SCA BB release 3.5.0 that relate to installation of the SCA BB console.

CSCsa94964

Uninstalling while GUI is open

Running the uninstaller while the SCA BB Console is open, can fail; however, no warning is given when starting the uninstallation. Close the SCA BB Console before running the uninstaller.

CSCsa94964

Must uninstall SCA BB Console before reinstalling it

You must uninstall the SCA before reinstalling it. Do not install the SCA on top of an existing installation.

CSCsc32003

Network Navigator configuration not removed when SCA BB Console uninstalled

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

Workaround:

To clear these settings, manually delete the following folder:

C:\Documents and Settings\<username>\.scasbb300

Network Navigator

This subsection describes open caveats in SCA BB release 3.5.0 that relate to the Network Navigator.

CSCsa95657

Two identical devices can be created

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

Incorrect error message for failure to connect

If you mistakenly provide the IP address of a device of a different type (for example, adding an SCE but with the IP address of an SM) connecting to this device will fail; the error message that is issued does not correctly identify the problem.

CSCsv55906

Double default site in the Network Navigator

When upgrading from 3.1.7 to 3.5.0, the Network configuration is not automatically imported. You export, and then import. Once the import is complete, two default sites appear in the window.

N/A

Concurrent operations on the same SCE platform are not supported

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

Updating CM with service configuration values in a NAT environment

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 open caveats in SCA BB release 3.5.0 that relate to the Service Configuration Editor.

CSCsx17491

Opening old PQB files (prior to 3.0.0) not supported in 3.5.0

PQB files that were created using SCA BB releases prior to 3.0.0 might not open in SCA BB release 3.5.0.

Workaround: Install SCA-BB 3.1.7, open the PQB and save it to the disk. You can then open it in SCA-BB 3.5.0.

N/A

New protocols not assigned automatically to services in old PQB files

When upgrading old PQB files, new protocols do not get assigned to any service. Signature-based protocols that are not assigned to a service are classified as Generic TCP, even if the flow itself is UDP.

Workaround:

Manually assign protocols to a service using the SCA.

Subscriber Manager GUI

This subsection describes open caveats in SCA BB release 3.5.0 that relate to the Subscriber Manager GUI.

CSCsw79014

SCA BB Subscriber Manager GUI - Many issues

The following issues with the SM Client GUI make it practically unusable:

- CSCsr09226 - 3.5.0-GUI - when using a VLAN SM GUI and changing a subscriber name, it freezes and the subscriber is removed (SM)
- CSCsw18320 - 3.5.0-SM GUI - subscriber details are not refreshed automatically
- CSCsj45511 - 3.1.5LA-GUI - the window freezes and you cannot work with the Subscriber Manager
- CSCsh57287 - GUI - the SM GUI is not up to date with SM DB
- CSCso30235 - Exporting subscribers fails with GUI 3.1.5 and SM 3.1.0
- CSCsi03280 - SM GUI can be connected to an SCE

- CSCsh96714 - SM GUI - when changing the subscriber domain, there is a logic problem
- CSCsh57286 - GUI - an SM GUI error appears when searching for a subscriber and the DB is empty
- CSCsl48003 - SCABB-SM GUI - a faulty radio button operation - adds VLAN and IP per subscriber
- CSCsl16383 - GUI - when adding a subscriber to the SM GUI there should be length limitation
- CSCsl47880 - SCABB-SM GUI does not allow adding a subscriber with more than 40 characters

Reporter

This subsection describes open caveats in SCA BB release 3.5.0 that relate to the Reporter.

N/A

Reporter sometimes shows service number instead of service name

In unusual circumstances, the Reporter shows some service numbers instead of the symbolic name.

The problem occurs after a policy has been applied to an SCE platform via the SCA BB Console, modified (by renaming, adding, or deleting services) and then reapplied.

This occurs only in SCA BB 3.0.5.

Workaround:

Save the service configuration and close the SCA BB Console, then reopen the Console and apply the service configuration.

Configuration Management

This section describes open caveats in SCA BB release 3.5.0 that relate to configuration management.

- General, page 16
- Service Configuration API, page 17

General

This subsection describes open caveats in SCA BB release 3.5.0 that relate to general issues concerning configuration management.

N/A

SCE log and SNMP traps when a service configuration is applied

Apply operations are logged in the SCE user log, with the origin file name and host. This can be viewed in SCE CLI in the following manner:

```
#more user-log
...
2005-12-18 10:20:54 | INFO | CPU #000 | Engage Policy Applied:
username@hostname/64.103.125.159, filename.pqb, Fully-Functional, 6(+1)Packages, 38
Services
...
```

The SCE also generates an SNMP trap with a similar message after a service configuration is applied.

Service Configuration API

This subsection describes open caveats in SCA BB release 3.5.0 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 SCA BB 3.0.0, to accommodate new product naming conventions. Nevertheless, the older API classes and methods can still be used.

Note, however, that the Service Configuration Editing API in SCA BB 3.0.0 has been significantly changed, and is generally incompatible with 2.5.

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 2.5 formats.

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.