Release Notes for Cisco Service Control Application Suite for Broadband (SCA BB) 2.5.10

March 15, 2006

Release Notes for Cisco Service Control Application Suite for Broadband (SCA BB) 2.5.10

Supports: SCA BB 2.5.10, SCA BB 2.5.9, SCA BB 2.5.8, SCA BB 2.5.7, SCA BB 2.5.6, SCA BB 2.5.5, SCA BB 2.5.2, SCA BB 2.5.1, SCA BB 2.5

OL-7082-08

These release notes for the Cisco SCA BB describe the enhancements provided in Cisco Release 2.5.10. These release notes are updated as needed.

For a list of the caveats that apply to Cisco Release SCA BB 2.5.10 see Open Caveats.

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

Contents

Introduction

Cisco is proud to release version 2.5.10 of its Service Control Application for Broadband (SCA BB).

Release 2.5.10 of SCA BB is a point release of SCA BB 2.5. It includes functional enhancements, as well as solutions for various caveats that were identified as part of Cisco's on-going internal testing and during our interaction with our customers.

This document outlines the functional enhancements to SCA BB and assumes 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.

Release 2.5.10

This section provides information on maintenance release 2.5.10, including compatibility information, capacity information, resolved issues, and new features and protocols.

Functional Enhancements

Protocol Support

The following table describes the new protocols that were added in 2.5.10. Note that some of these protocols are also available in the latest 2.5.9 protocol pack.

Table 1 New Protocols in SCA BB 2.5.10

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
Dijjer	56	A P2P protocol	Assigned to the default P2P service.
Exosee	57	A P2P protocol	Assigned to the default P2P service.
PeerEnabler	58	A P2P protocol	Assigned to the default P2P service.
Furthur	59	A P2P protocol	Assigned to the default P2P service.
Kontiki	60	A P2P protocol	Assigned to the default P2P service.

Note When upgrading old PQB files, new protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as generic TCP. To fix this, manually assign the new protocols to a service using the SCA BB Console.

This release also includes updates for the following protocols:

- BitTorrent–New signatures
- Skype–New signatures
- Winny–Improved signature intended to resolve a few false-detection cases. The old Winny1 signature is disabled and can be revived if needed.

Resolved Caveats

The following caveat is resolved in this release:

Inaccurate Call Duration Report for SIP and H323

- Cisco Number CSCsc41280

Reports of aggregated voice call duration of SIP and H323 might show higher aggregated duration than the actual duration, because at certain (common) cases, session aging time is regarded as part of the call. The inaccuracy is about 240 additional seconds per SIP/H323 session. It is hard to estimate the level of overall inaccuracy.

This issue is resolved in this release.

Inaccurate Global and Package Concurrent Sessions Report

- Cisco Number CSCsd92763

The concurrent calls/sessions reported in the "Global/Package Concurrent calls/sessions" reports were not accurate, since these reports were incorporating counts of all sessions seen on the specific service, and not just call sessions.

This issue is resolved in this release.

Compatibility Information

SCA BB 2.5.10 should be used with the following components:

- SCOS 2.5.10
- SCMS-SM 2.5.5, 2.5.6, 2.5.7, 2.5.8
- SCMS-CM 2.5.5, 2.5.8

Capacity Information

SCA BB 2.5.10 supports the following flow and subscriber capacity numbers for the two main capacity options.

Table 2 Flow and Subscriber Capacity in SCA BB 2.5.10

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000) **DEFAULT**	80,000	1.7M [850K bi-directional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U) **DEFAULT**	40,000	1.7M [850K bi-directional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bi-directional]
SCE1000_1.5U (EngageDefaultSCE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	1M [500K bi-directional]

Release 2.5.9

This section provides information on maintenance release 2.5.9, including compatibility information, capacity information, resolved issues and new features and protocols.

Functional Enhancements

Protocol Support

The following table describes the new protocols that were added in 2.5.9. Note that some of these protocols are also available in the latest 2.5.8 protocol pack.

Table 3 New Protocols in SCA BB 2.5.9

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
HTTP Tunnel	50	Standard HTTP used for tunneling	Added to a new "Tunneling" service.

Note When upgrading old PQB files, new protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as generic TCP. To fix this, you should manually assign the new protocols to a service using the SCA BB Console.

SIP: Distinguishing between Voice and Video

A new RDR named Media-Streaming Flow RDR is generated upon termination of each SIP Media RDR. The RDR fields are listed in the following table:

Table 4 Media-Streaming Flow RDR Fields

RDR Field	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see the *Cisco SCA-BB Reference Guide*
PACKAGE_ID	UINT16	A universal field; see the *Cisco SCA-BB Reference Guide*
SERVICE_ID	UINT32	A universal field; see the *Cisco SCA-BB Reference Guide*
PROTOCOL_ID	INT16	A universal field; see the *Cisco SCA-BB Reference Guide*
SERVER_IP	UINT32	A universal field; see the *Cisco SCA-BB Reference Guide*

RDR Field	Type	Description
SERVER_PORT	UINT16	A universal field; see the *Cisco SCA-BB Reference Guide*
CLIENT_IP	UINT32	A universal field; see the *Cisco SCA-BB Reference Guide*
CLIENT_PORT	UINT16	A universal field; see the *Cisco SCA-BB Reference Guide*
INITIATING_SIDE	UINT8	A universal field; see the *Cisco SCA-BB Reference Guide*
REPORT_TIME	UINT32	Ending Timestamp (GMT time) of the transaction reported in this RDR. The field is a UNIX time_t format, that is, the number of seconds since 1 January 1970.
SEC_DURATION	UINT32	Duration, in seconds, of the transaction reported in this RDR.
FLOW_UPSTREAM_VOLUME	UINT32	Upstream volume of the admitted transaction, in bytes.
FLOW_DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the admitted transaction, in bytes.
IP_PROTOCOL	UINT8	IP protocol type
FLOW_TYPE	UINT8	1 – audio 2 - video
SESSION _ID	UINT32	Internal Session ID

This RDR is disabled by default, and can only be enabled using ROOT CLI, as follows:

```
SCE2000#>configure
SCE2000(config)#>interface LineCard 0
SCE2000(config if)#>tunable GT_REP_enableMediaFlowReport value true
SCE2000(config if)#>exit
SCE2000(config)#>exit
SCE2000#>copy running-config application startup-config application
```

Note that when a user performs a Video chat, two RDRs are generated; one for Video, and one for Voice. A correlation between the two is required, if the user wants to ignore the Voice RDR that is correlated with the Video one.

Resolved Caveats

The following caveats are resolved in this release:

GC Convergence on Time Frame changes

- Cisco Number CSCsb28481

In previous releases, when different global BW limitations were defined for the same service on different time frames, the convergence of the Global Controller to the new global BW limit when time-frames changed was slow, and usually started with a BW spike. This problem was evident in Global BW per Service reports.

The cause of this behavior is that whenever time frames changed, flows were gradually assigned to a new GC. This controller then restarted the BW convergence process, regardless of the state of the previous GC.

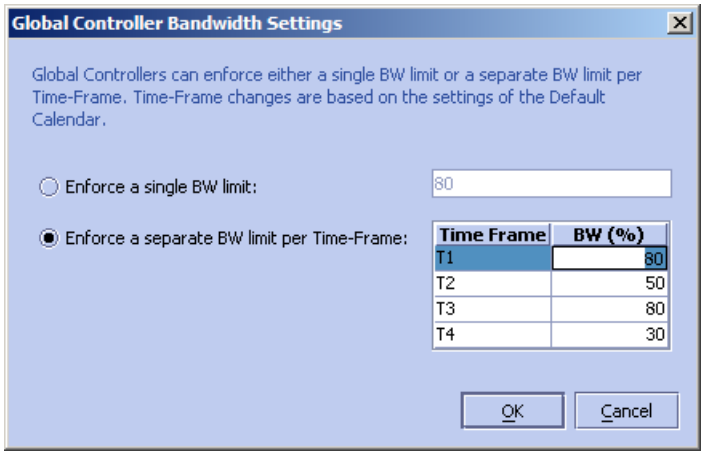
In this release, this is solved as follows: Flows are not re-assigned to a new GC on time-frame change, and instead, the GC is assigned a new BW value. For each GC, the user can define different BW limits separately for each of the four time frames.

In the service configuration editor, the Global Controller Settings window was enhanced to allow time-based GC values.

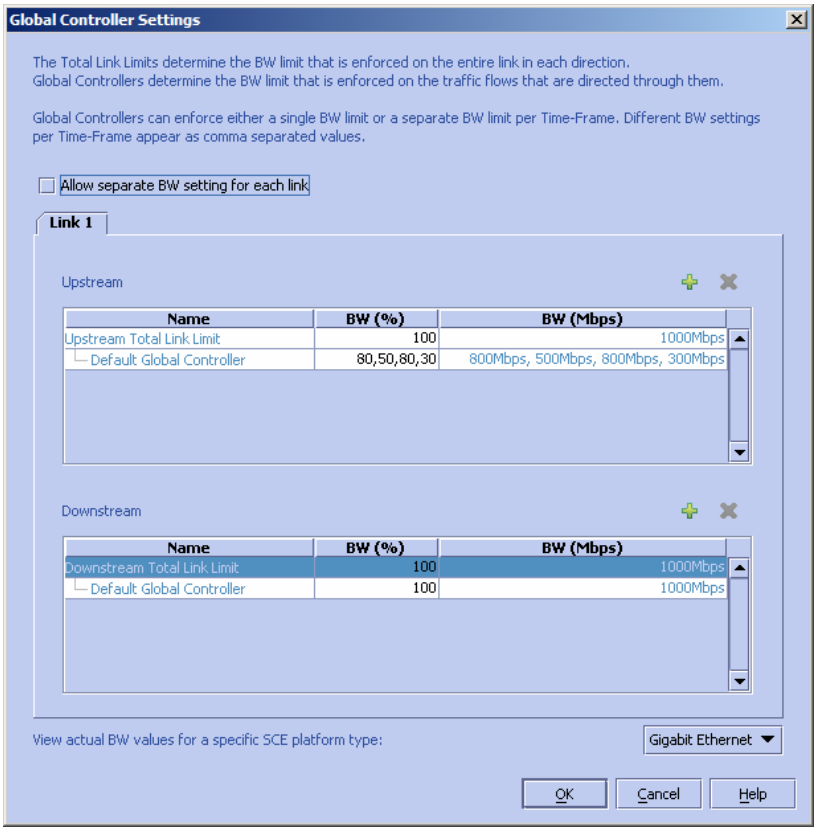
To enter separate GC BW limits per time frame, follow these steps:

Step 1. In the Global Controller Settings Window, click the "BW (%)" cell to edit the value. The Global Controller Bandwidth Settings Dialog appears.

Step 2. In the Global Controller Bandwidth Settings Dialog, select "Enforce a separate BW limit per Time-Frame", and enter a BW limit for each time frame.



The “BW (%)" cell of the Global Controller Settings Window displays four different BW limits, one for each time frame, as illustrated in the following figure.



Once the service configuration is applied to the SCE platform, time-based GC values are always updated to hold the values according to the current time frame.

Note the following:

- Although 10 calendars are supported, time-based GC values are only affected by the current time frame of the Default Calendar, and are not affected by other calendars.
- Time-based GC values are not affected by the configuration of time-based rules. The user may still use time-based rules to direct a service to a different GC in each time frame.
- When the application system mode is *report-only* or *transparent*, GC values are always set to 100% (unlimited), and the configured values (and time-based values) are ignored.

Note Important note for users who experienced this problem in previous releases, and are upgrading to this release:
Time-based rules in old PQBs, which use separate GCs per time frame, are not automatically transformed to the new explicit configurations. To upgrade such PQBs, the GC time-based values should be configured, and the time-based rules should be removed.

Inaccuracy in Reports That Include Total Number of Subscribers

- Cisco Number CSCsc87746

Demographic reports on different services showed different numbers of total active subscribers at the same time. Specifically, reports on services with low activity also showed an incorrectly low number of active subscribers. This issue is fixed in this release.

Misclassification of HTTP with Jakarta User-Agent as Gnutella

- Cisco Number CSCsc95139

HTTP flows that had "Jakarta" in their user-agent were misclassified as Gnutella. This issue is fixed in this release.

Flows Starting with 'GET' (e.g. HTTP 0.9) not Reported or Controlled

- Cisco Number CSCsd17487

Flows in which the first payload packet starts with 'GET', but does not match HTTP 1.0/1.1 pattern, sometimes were not reported or controlled by the SCE platform. This issue is fixed in this release.

Misclassification of P2P Traffic on Well-Known Ports of Other Protocols

- Cisco Number CSCsd14658

P2P traffic on well-known ports of other protocols, such port 1720 (H323) and port 554 (RTSP) was not classified as P2P. This issue is fixed in this release.

Protocol Enhancements

This release includes enhanced signatures for the following protocols:

- Skype: New Skype version (1.4)
- PPLive: New client version

Compatibility Information

SCA BB 2.5.9 should be used with the following components:

- SCOS 2.5.9
- SCMS-SM 2.5.5, 2.5.6, 2.5.7, 2.5.8
- SCMS-CM 2.5.5, 2.5.8

Capacity Information

SCA BB 2.5.9 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 5 Flow and Subscriber Capacity in SCA BB 2.5.9

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000) **DEFAULT**	80,000	1.7M [850K bi-directional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U) **DEFAULT**	40,000	1.7M [850K bi-directional]
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bi-directional]
SCE1000_1.5U (EngageDefaultSCE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	1M [500K bi-directional]

Release 2.5.8

This section provides information on maintenance release 2.5.8, including compatibility information, capacity information, resolved issues and new features and protocols.

Functional Enhancements

Protocol Support

The following table describes the new protocols that were added in 2.5.8. Note that some of these protocols are also available in the latest 2.5.7 protocol pack.

Table 6 New Protocols in SCA BB 2.5.8

Protocol Name	Protocol ID	Description	Changes to the Default Service Configuration
BaiBao	43	BaiBao is a P2P protocol.	Assigned to the default P2P service
PPLive	44	PPLive is protocol for free online TV	Assigned to the default P2P service
Yahoo Messenger VoIP	45	Yahoo Messenger VoIP is a flavor of SIP, similar to Vonage.	Assigned to the default Voice service
Mobile MMS	46	Multimedia Messaging Service, for sending text messages on mobile devices	Assigned to the default Instant Messaging service
DNS	47	Domain Name Service Protocol	Assigned to the default Net-Admin service
UC	48	UC Instant Messenger	Assigned to the default Instant Messaging service
PPStream	49	A P2P Streaming application	Assigned to the default P2P service
Thunder	50	A Download Accelerator	Assigned to the default P2P service
Poco	51	POCO P2P application	Assigned to the default P2P service
QQ	52	QQ Instant Messenger	Assigned to the default Instant Messaging service
SSDP	53	Simple Service Discovery Protocol used by P2P apps	Assigned to the default P2P service
NTP	54	Network Time Protocol	Assigned to the default Net-Admin service

Mobile MMS Classification

Mobile MMS classification that was added in release 2.5.8 has the following limitations:

- Only MMS over HTTP is detected. MMS over WAP is not detected.
- Only sending of MMS messages ("POST") is classified as Mobile MMS.

To classify downloads of MMS messages ("GET") as Mobile MMS, the user should perform the following configuration steps in the SCA BB Console:

Step 1. Create a new Host List named "MMS Server";

Step 2. Add the host name of the provider's MMS server to the "MMS Server" host list.

Step 3. Add a service-element to the "Instant Messaging Service" that is made of the "HTTP Browsing" protocol and the "MMS Server" host list.

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 generic TCP. To fix this, manually assign these protocols to a service.

Resolved Caveats

The following caveats are resolved in this release:

Voice Report Inconsistency

- Cisco Number CSCsb67206

Previously, for the VoIP service, the number of calls reported was too high for the reported bandwidth.

This issue is resolved in this release.

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

- Seconds – Dedicated to VoIP reports. Shows the aggregated call seconds. (Appears also in Party Usage Report)
  - VoIP: Counts only VoIP calls and not control flows, and does not count aging time.
  - Non-VoIP services: counts aggregate session seconds.
- Concurrent Session – Number of concurrent sessions.
  - Counts all sessions, not different for VoIP.
  - Session that ends by aging is still being counted at time of aging.
  - Not aggregated, shows temporary value at time of report.
- Concurrent Active Subscribers – Shows number of subscribers that have a session open for the service reported.
  - Counts all sessions, not different for VoIP.
  - Not aggregated, shows temporary value at time of report

Quota Reset When Subscriber Becomes Introduced (Pull Mode)

- Cisco Number CSCsb78012

When a subscriber was introduced after being managed as anonymous by the application, his quota was reset.

This has two undesirable results under the above circumstances:

- An externally provisioned subscriber would loose all his quota immediately after login
- Any subscriber would lose his state as preserved in the SM

This issue is resolved in 2.5.8.

Quota Reset on Package-Update (Pull Mode)

- Cisco Number CSCsb78012

If a subscriber moved to an externally-provisioned package, his buckets were reset. However, the reset voided the quota-update.

This issue is resolved in 2.5.8.

VoIP Transaction Usage RDR – Clarification

Following is a clarification regarding the semantics of fields in the VoIP Transaction Usage RDR (tag 4042321940), which are extracted from the Voice RTCP flow:

Packet Loss

This field is taken from RTCP field *'fraction lost'*. It is the average value of all RTCP packets seen during the flow life for the specified direction. The value is the numerator of a fraction whose denominator is 256. To get the packet loss value as percentage, divide the value by 2.56.

Average Jitter

This field is taken from the RTCP field '*interval jitter'*. The reported value is the average value of all RTCP packets seen during the flow life for the specified direction. This value is multiplied by the NTP timestamp delta (middle 32 bits) and divided by the RTP timestamp delta, to convert it to normal time units. These two timestamps are also taken from the RTCP packet. The reported value is the average jitter in units of 1/65536 second. To convert to milliseconds divide by 65.536.

See RFC 1889 for further information about the RCP/RTCP standard.

Enhanced Capacity in Handling BitTorrent Traffic

- Cisco Number CSCsc41572

This feature (see Enhanced Capacity In Handling BitTorrent) was not functioning correctly.

This issue is resolved in 2.5.8.

Protocol Fixes

This release includes enhanced signatures for the following protocols:

- Skype
- Morpheus (Neonet)
- BitTorrent over UDP
- MGCP
- Share over UDP
- SIP

In addition, the following classification issues have been resolved

- DHCP misclassified as Manolito.
- Morpheus misclassified Winny
- DNS misclassified as Winny or eDonkey
- PalTalk misclassified Winny

Default Service Rule Refers to an Invalid BW Controller

- Cisco Number CSCsc44706

In previous releases, the Default Service Rule in each package contained invalid mapping of traffic to Subscriber BW Controller. This might have resulted in invalid BW control on traffic that is controlled by the default service rule.

This issue is resolved in 2.5.8. Old QPB files are automatically repaired when used in 2.5.8. The following messages may appear to indicate the correction:

```
Warning: The default rule for service "Default Service" in package "Default
Package" had an invalid Downstream Post-Breach BWC reference. It has been
rerouted to the default BWC.
Warning: The default rule for service "Default Service" in package "Default
Package" had an invalid Downstream Pre-Breach BWC reference. It has been
rerouted to the default BWC.
Warning: The default rule for service "Default Service" in package "Unknown
Subscriber Traffic" had an invalid Downstream Pre-Breach BWC reference. It has
been rerouted to the default BWC.
Warning: The default rule for service "Default Service" in package "Unknown
Subscriber Traffic" had an invalid Downstream Post-Breach BWC reference. It
has been rerouted to the default BWC.
```

Protocol Pack Installation Enhancements and Fixes

A number of issues were resolved and enhancements added to the process of installing protocol packs using the SERVCONF utility to make the process more reliable.

Among these enhancements is that SERVCONF can now be used with both Java 1.5 and 1.4. Note that the SIGCONF utility still requires Java 1.4.

Compatibility Information

SCA BB 2.5.8 should be used with the following components:

- SCOS 2.5.8
- SCMS-SM 2.5.5, 2.5.6, 2.5.7, 2.5.8
- SCMS-CM 2.5.5, 2.5.8

Upgrade Note

When upgrading from 2.5.7 with the latest protocol pack to 2.5.8, the following should be noted:

- When using 2.5.8 to open a PQB file that was created with the latest 2.5.7 protocol pack, some protocol IDs are changed automatically. The following messages may appear to indicate the change:

```
Protocol ID of BaiBao changed from 80 to 43
Protocol ID of PPLive changed from 81 to 44
Protocol ID of UC changed from 89 to 48
Protocol ID of PPStream changed from 84 to 49
Protocol ID of Thunder changed from 87 to 50
Protocol ID of NTP changed from 86 to 54
Protocol ID of SSDP changed from 85 to 53
Protocol ID of QQ changed from 88 to 52
Protocol ID of DNS changed from 82 to 47
```

- 2.5.8 does not use the "Default DSS" that was installed for 2.5.7.
- If a protocol pack for 2.5.8 is available, it should be installed on top of a 2.5.8 installation. Do not install a 2.5.7 protocol pack on top of 2.5.8.

Capacity Information

SCA BB 2.5.8 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 7 Flow and Subscriber Capacity in SCA BB 2.5.8

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000) **DEFAULT**	80,000	1.7M [850K bi-directional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U) **DEFAULT**	40,000	1.7M [850K bi-directional]

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE1000_2U (SubscriberLessSCE1000_2U)	1,000	2M [1M bi-directional]
SCE1000_1.5U (EngageDefaultSCE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000_1.5U (SubscriberLessSCE1000)	1,000	1M [500K bi-directional]

New Functionality in Release 2.5.7

This section provides information on maintenance release 2.5.7, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features

Protocol Signature Distribution

Cisco periodically publishes signature update packs that include new and improved protocol signatures for SCA BB. A typical signature update is a file containing signatures for detecting protocols including network traffic worms and popular peer-to-peer applications. When loaded into SCE platforms, these signatures improve the SCA BB classification capabilities with minimal SCE service downtime.

SCA BB 2.5.7 provides an automatic procedure for distributing signature updates to multiple SCE platforms. An additional procedure is provided to automatically update existing service configuration files (PQB files).

Additional information on obtaining signature update packs and the automatic distribution is available in the application notes that accompany this release.

Cisco SCE as an Intercept Application Manager in PCMM Architecture

SCA BB 2.5.7 is accompanied by an application note that provides an overview of the concept of implementing a PCMM Intercept Application Manager using a Cisco SCE platform and a guide for setting up such a demo.

The application note focuses on operating the SCE IAM based on SCA BB 2.5.7 in conjunction with the Camiant PCMM Policy Server. The integration of SCA BB and Camiant is based on translating QoS Request/Delete RDRs from the SCE platform into PCMM requests sent to Camiant servers. The translation and communication with the Camiant server is performed by a PCMM adapter, which is installed as a patch on the existing CM 2.5.5.

Protocol Support

DINGOTEL

A new protocol, whose protocol ID is 42. In the default service configuration, DingoTel protocol is assigned to a new DingoTel service under the VoIP service.

BITTORRENT

Added detection of Azureus BitTorrent client in the BitTorrent signature.

SHARE

Improved signature for the Share P2P protocol is available in the latest signature-update for Asia-Pacific region (susap.dss).

Change in Zeroing Mechanism of Subscriber Usage RDRs

Subscriber Usage Zeroing RDRs are no longer generated in SCA BB 2.5.7. This change should have no effect on systems using the Subscriber Usage RDRs, as these RDRs only indicate periods of subscriber inactivity. A workaround is available and can be used when Zeroing RDRs must be turned on.

There is no change in the zeroing mechanism of Link Usage RDRs, Package Usage RDRs and Real-time Subscriber Usage RDRs used by the Reporter.

Dependency of Behavioral Classification on Subscriber Integration Mode – A Clarification

Classification of some of the P2P protocols in the SCA BB, such as ***Skype***, ***Warez***, and ***Winny 2,*** makes use of the heuristic method called "behavioral classification". This method maintains a record of previous network usage patterns of the subscriber in order to better classify its current network traffic. This method relies on the system's subscriber integration mode, and specifically has limitations when a subscriber is defined as a large IP range. The subscriber represents many home users rather than one, which may lead to misclassification of the behavioral mechanism.

When facing this problem in installations where a subscriber is defined as a large IP range, there are two possible solutions:

- Move to anonymous subscriber mode, or
- Disable the Behavioral Classification Mechanism

To disable the Behavioral Classification Mechanism:

Step 1. Login to the SCE Platform a root ("enable 15")

Step 2. Use the following CLI sequence:

```
#>interface LineCard 0
(config) #>tunable PL_SKYPE_USE_BEHAVIORAL_DB value FALSE
(config if) #>tunable PL_SKYPE_USE_BEHAVIORAL_DB value FALSE
(config if) #>tunable PL_SKYPE_USE_BEHAVIORAL_DB value FALSE
(config if) #>exit
(config) #>exit
#>copy running-config-application startup-config-application
```

Preventing Loss of RDRs on the Collection Manager – Recommended Configuration Change

To prevent loss of RDRs, make the following configuration changes on the CM:

Step 1. Edit the file ~pcube/pump/config/pump.conf

Locate the "buffer" section. It looks like this:

```
[buffer]
size = 4096
time = 2000
file limit = 10000
```

Step 2. Change the "size parameter to 128000, like this:

```
[buffer]
size = 128000
time = 2000
file limit = 10000
```

Step 3. Save the file and restart the CM for the change to take effect.

Resolved Caveats

Caveats resolved in this release:

- The actual RDR rate enforced on Subscriber Usage RDRs was lower than the configured rate.
- Skype concurrent calls counter showed incorrect values that are greater than the actual number of calls.
- A subscriber that was mapped to a non-existing package was still mapped to the default package after the non-existing package is added.
- Some gaming protocols and DNS flows were misclassified as Winny protocol.
- Reporter: Low performance of the "Hourly Usage Volume Sessions" reports.

Compatibility Information

SCA BB 2.5.7 should be used with the following components:

- SCOS 2.5.7
- SCMS-SM 2.5.2, 2.5.5, 2.5.6, 2.5.7

- SCMS-CM 2.5.5

Capacity Information

SCA BB 2.5.7 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 8 Flow and Subscriber Capacity in SCA BB 2.5.7

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000) **DEFAULT**	80,000	1.7M [850K bi-directional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U) **DEFAULT**	40,000	1.7M [850K bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	2M [1M bi-directional]
SCE1000 (EngageDefaultSCE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000 (SubscriberLessSCE1000)	1,000	1M [500K bi-directional]

New Functionality in Release 2.5.6

This section provides information on maintenance release 2.5.6, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features

New Protocols and Applications

NEW BITTORRENT CLIENT: EXEEM

The BitTorrent protocol signature was enhanced to detect the Exeem P2P client. Exeem traffic is now classified as BitTorrent and is mapped to the appropriate service.

NEW VOIP PROTOCOL: SKINNY

Cisco Skinny VoIP Protocol is now detected. In the default service configuration, Skinny is defined as a sub service of the VoIP service. It also appears in VoIP Reports.

NEW INSTANT MESSAGING PROTOCOL: YAHOO MESSENGER

Yahoo Messenger protocol signature was added. In the default service configuration, it is defined under the Instant Messaging service.

Enhanced Capacity in Handling BitTorrent Traffic

BitTorrent clients use a very large number of concurrent connections for file sharing, though most of the connections are inactive most of the time. This situation poses a challenge to the SCE in networks where BitTorrent is the prevailing protocol, as the SCE might enter a state of flow memory shortage or incorrectly classify BitTorrent traffic as "Generic".

This release introduces an optimized solution for enhanced capacity in handling BitTorrent traffic. This enhancement ensures that inactive connections consume significantly less SCE resources, while not degrading the quality of traffic classification.

Resolved Caveats

Caveats resolved in this release:

- Call duration and number of concurrent calls reported incorrectly for Skype (but see the "Skype Reporting Limitations" note under the Open Caveats section.)
- MIB counters of active subscribers and concurrent sessions might show incorrect values
- Number of active subscribers reported incorrectly for SMTP

Compatibility Information

SCA BB 2.5.6 should be used with the following components:

- SCOS 2.5.6 (previously P-Cube SEos)
- SCMS-SM 2.5.2, 2.5.5, 2.5.6 (previously P-Cube smartSUB Manager)
- SCMS-CM 2.5.5 (previously P-Cube Data Collector).

Capacity Information

SCA BB 2.5.6 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 9 Flow and Subscriber Capacity in SCA BB 2.5.6

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000) **DEFAULT**	80,000	1.7M [850K bi-directional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U) **DEFAULT**	40,000	1.7M [850K bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U)	40,000	2M [1M bi-directional]
SCE1000 (EngageDefaultSCE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000 (SubscriberLessSCE1000)	1,000	1M [500K bi-directional]

New Functionality in Release 2.5.5

This section provides information on maintenance release 2.5.5, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features and Protocols

Reporting Enhancements

Release 2.5.5 introduces several enhancements in the area of analysis and reporting. These enhancements, which are described in details below, are reflected in new Reports, as well as in a new structure of Report Groups in the reporter (see more details in the *SCA BB 2.5.5 User Guide*).

Following is the list of Report Groups in the 2.5.5 Reporter:

- Global Monitoring
- Package Monitoring (previously found under global monitoring)
- Subscriber Monitoring
- Traffic Discovery – Statistics
- Demographic Data and Service Popularity (a new group, described below)
- Web and Streaming (previously found under Traffic Discovery – Application Popularity)
- Mail and News (previously found under Traffic Discovery – Application Popularity)
- P2P
- VoIP (a new group, described below)
- Malicious Traffic (a new group, described below)

VoIP Reports

Reporting on VoIP traffic was enhanced as follows:

- Improved VoIP protocols support: Added support for **MGCP** protocol, and updated **Skype** signature
- New VoIP specific reports, which provide information on network traffic generated by VoIP applications (currently these are H323, SIP, Vonage, Skype and MGCP). These reports include: Call Minutes per VoIP Service, Concurrent Calls per VoIP Service, Top SIP Domains, and Top Talkers.

DEMOGRAPHIC REPORTS

A new group of reports was added, to provide information on demographic data and service popularity. These reports include: Active Subscribers per Service, Service Popularity among Subscribers, Relative Consumption of Top Subscribers, and more.

MALICIOUS TRAFFIC REPORTS

A new group of reports was added, to provide information on malicious network traffic, such as Denial-of-Service attacks and Internet Worms distribution. These reports include: Top DoS Attacked Hosts, Infected Subscribers, Top Scanning/Attacking Hosts, and more.

TRAFFIC DISCOVERY ENHANCEMENTS

Traffic discovery enhancements aim to minimize the amount of "generic" traffic and increase overall granularity of usage reports in common use cases. This is achieved by:

- A new default service configuration (PQB). The default PQB now includes new predefined services for gaming, network administration, instant messaging and VoIP applications, as well as more granular service definitions for other popular applications, such as P2P, email, streaming, etc.
  Note that these enhancements are made in the default PQB, are therefore only applicable for newly created PQB files, but not for PQB files that are upgrade from previous versions.
- The Reporter now allows a separate "Top Ports" Reports for TCP and UDP ports.

NEW NETWORK USAGE METRICS

The SCE application maintains the following network usage metrics (in addition to existing volume and number-of-sessions metrics):

- Concurrent Sessions per Service (maintained in Package and Link scopes)
- Concurrent Active Subscribers per Service (maintained in Package and Link scopes)
- Aggregated Session Duration per Service (in seconds, maintained in Subscriber, Package and Link scopes)

These metrics are available as new fields in Usage RDRs, as well as new counters in SCA BB SNMP MIB.

Quota Provisioning Enhancements

Quota Provisioning (QP) feature has been enhanced in 2.5.5 as follows.

- Quota modifications (addQuota, setQuota) can take place even when the subscriber is not introduced in the SCE platform, or is inactive.
- Quota modifications can be queued in the SM.

No changes were made to the actual QP API interfaces. See more details in the *SCA BB 2.5.5 Programmer's Guide*.

QoS Request/Delete RDRs for Real-time Signaling

QoS Request/Delete RDRs are generated at the beginning/end of a flow, according to the flow's service and subscriber-package configuration. These RDRs are used to signal external systems of setup and teardown on service flows, to enable real-time actions across the network. These new RDRs are intended to be used by external frameworks (such as PCMM compliant systems) to allocate QoS for flows that are classified by the SCE.

See more details about these RDRs in the *SCA BB 2.5.5 User Guide (RDR Appendix)*.

Cisco Product Branding

Release 2.5.5 introduces product-branding updates, to indicate the transition from "P-Cube Engage" to "Cisco SCA BB". Some of the more noticeable changes are:

- Console start menu location: Start➔Programs➔Cisco SCAS➔SCA BB 2.5.5
- Reporter start menu location: Start➔Programs➔Cisco SCAS➔SCAS Reporter 2.5.5
- GUI client's default installation location: C:\Program Files\Cisco SCAS\SCA BB 2.5.5
- New GUI splash screens.
- Default password for connecting the SCA BB Console to the SCE was changed.

Resolved Caveats

Caveats resolved in this release:

- [14149] Importing services fails when child service appears before parent service
- [14128] PQI: Engage pre-configured subscriber templates lost after SCE reload
- [14072] SCE Application's system mode during apply of service configuration
- QP C API cannot update 16 quota buckets

Compatibility Information

SCA BB 2.5.5 should be used with the following components:

- SCOS 2.5.5 (previously P-Cube SEos)
- SCMS-SM 2.5.2, 2.5.5 (previously P-Cube smartSUB Manager)
- SCMS-CM 2.5.5 (previously P-Cube Data Collector).

Capacity Information

SCA BB 2.5.5 supports the following flow and subscriber capacity numbers, for the two main capacity options.

Table 10 Flow and Subscriber Capacity in SCA BB 2.5.5

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSCE2000) **DEFAULT**	80,000	1.7M [850K bi-directional]
SCE2000 (SubscriberLessSCE2000)	2,000	2M [1M bi-directional]
SCE1000_2U (EngageDefaultSCE1000_2U) **DEFAULT**	40,000	1.7M [850K bi-directional]
SCE1000 (EngageDefaultSCE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000 (SubscriberLessSCE1000)	1,000	1M [500K bi-directional]
SE100 (EngageDefaultSE100) **DEFAULT**	10,000	200K [100K bi-directional]
SE100 (SubscriberLessSE100)	1,000	200K [100K bi-directional]

New Functionality in Release 2.5.2

This section provides information on maintenance release 2.5.2, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features and Protocols

New P2P Protocol

Support added for Ares/Warez P2P protocol. The signature for this protocol is available in this release as a signature update script, which needs to be loaded into the service configuration (PQB file).

Winny Classification Settings

The Winny P2P protocol is used by the Winny file-sharing application. This application is popular in Japan. This release provides two inspection modes for classification of the protocol:

- ***Default***—Suitable for networks in which little Winny traffic is expected. This is the common case in all geographies except Japan.
- ***Detailed***—Suitable for networks where Winny traffic is expected to be common. This should be the case in Japanese networks only.

The correct setting should be used to optimize the deep packet inspection engine's classification and performance and should be set according to the environment where it is installed.

Activating Detailed Winny Inspection Mode:

The detailed Winny inspection mode is activated by running a CLI script on the SCE. The script file, *winny2.cli*, is included in this release. To run the script, follow these steps:

(1) Login to the SCE CLI as root ("enable 15");

(2) Upload the file *winny2.cli* to the SCE file system

(3) In the SCE CLI prompt, type:

```
run script winny2.cli
```

Resolved Caveats

Caveats resolved in this release:

- At rare occasions, HTTP is classified as Gnutella.

  Note that with this fix, HTTP is classified correctly, but Gnutella classification now requires that the latest DSS be applied as part of the PQB file.

- [14071] While a service configuration is applied, system mode changes to “transparent” for a short period of time, causing a considerable amount of traffic not be reported in usage RDRs, and not be controlled by policy rules, during that period.
- [13520] Unreasonable volume peaks in usage RDRs, causing incorrect bandwidth reports in the Reporter.

Compatibility Information

SCA BB 2.5.2 should be used with the following components:

- SCOS 2.5.2 (previously P-Cube SEos)
- SCMS-SM 2.5.2 (previously P-Cube smartSUB Manager)
- SCMS-CM 2.5.1 (previously P-Cube Data Collector).

Capacity Information

SCA BB 2.5.2 supports the following flow & subscriber capacity numbers, for the two main capacity options.

Table 11 Flow and Subscriber Capacity in SCA BB 2.5.2

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSE2000) **DEFAULT**	80,000	1.4M [700K bi-directional]
SCE2000 (SubscriberLessSE2000)	2,000	2M [1M bi-directional]
SCE1000 (EngageDefaultSE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000 (SubscriberLessSE1000)	1,000	1M [500K bi-directional]
SCE100 (EngageDefaultSE100) **DEFAULT**	10,000	200K [100K bi-directional]
SE100 (SubscriberLessSE100)	1,000	200K [100K bi-directional]

New Functionality in Release 2.5.1

This section provides information on maintenance release 2.5.1, including compatibility information, capacity information, resolved issues and new features and protocols.

New Features and Protocols

P2P Protocol Support update

P2P support for the following applications was added:

- Soulseek Protocol Number 29
- iTunes Protocol Number 30
- Filetopia Protocol Number 31
- Napster Protocol Number 32
- Mute Protocol Number 34
- Nodezilla Protocol Number 35
- Waste Protocol Number 36

Resolved Caveats

The following issue has been resolved as part of the release:

- Packets dropped not in accordance with policy, due to incorrect assignment of priority: Corrected

Compatibility Information

SCA BB 2.5.1 should be used with the following components:

- SCOS 2.5.1 (previously P-Cube SEos)
- SCMS-SM 2.5.1 (previously P-Cube smartSUB Manager)
- SCMS-CM 2.5.1 (previously P-Cube Data Collector). N

Capacity Information

SCA BB 2.5.1 supports the following flow & subscriber capacity numbers, for the two main capacity options.

Table 12 Flow and Subscriber Capacity in SCA BB 2.5.1

Device (Capacity Option)	Number of Subscribers	Number of Flows
SCE2000 (EngageDefaultSE2000) **DEFAULT**	80,000	1.4M [700K bi-directional]
SCE2000 (SubscriberLessSE2000)	2,000	2M [1M bi-directional]
SCE1000 (EngageDefaultSE1000) **DEFAULT**	40,000	700K [350K bi-directional]
SCE1000 (SubscriberLessSE1000)	1,000	1M [500K bi-directional]
SE100 (EngageDefaultSE100) **DEFAULT**	10,000	200K [100K bi-directional]
SE100 (SubscriberLessSE100)	1,000	200K [100K bi-directional]

New Functionality in Release 2.5

New Features and Protocols

Session Quotas Not Supported

Revision 2.5.0 does not provide support for session quotas.

PQB File logging

The apply procedure logs the name of the PQB file on the SCE device it is applied to. Use **`more user-log | include "SCA BB Policy"`** on the SCE CLI to view list of policy files applied.

Important Note

In October 2004, P-Cube Inc. was purchased by Cisco Systems. P-Cube's products and technology are now part of Cisco's wide range of products and solutions for broadband service providers, and will complement the existing Cisco products with Service Control technology, allowing operators to increase visibility and control over network traffic and broadband subscribers' activity. Cisco Systems will continue support and development of the Service Control product line, and is committed to supporting both existing P-Cube customers and future customers of the Service Control technology.

The product-line has undergone revisions in naming to accommodate to standard Cisco naming.

Open Caveats

Traffic Analysis & Control Issues

Inaccurate BW Control when Using the Default Global Controller

- Cisco number: CSCsc35019

  The Default Global Controller (GC) might enforce inaccurate BW limit on the traffic that is assigned to it, due to the fact that additional uncontrolled traffic, such as traffic filtered by traffic filter rules, is also assigned to this GC.

  It is therefore recommended not to use this GC for BW control, and keep its BW limit set to 100%.

Top Subscriber Reports Show Unreasonable Bandwidth

- Cisco number: n/a

  Top subscriber reports might show unreasonably high bandwidth consumed by a subscriber. These reports are based on Subscriber Usage RDRs and the problem occurs because of an issue with the rate limit that is enforced on the generation of Subscriber Usage RDRs by the SCE application. When the rate limit on RDRs is too low, the reports are likely to show unreasonably high values.

  Workaround: To overcome this problem, it is recommended to disable the rate limit on Subscriber Usage RDRs. In SCA BB 2.5.7, the rate limit is disabled by setting the rate to 6000 or more RDRs per second. This value is configured in the SCA BB Console by selecting **Configuration** > **RDR Settings** > **Usage RDRs** > **Subscriber Usage RDRs**.

Skype Reporting Limitations

- Cisco number: CSCsb05427, CSCsb05425, CSCsb05422

SKYPE CALL DURATION INACCURACIES

Release 2.5.6 delivers a fix to the incorrect Skype duration reporting, which was introduced on the 2.5.5 release. However, 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/stop events detection can be delayed by 30-60 seconds, and a single call duration measurement may involve inaccuracy of +/-30 seconds or 20% (the larger).
- Skype call that is carried over two connections (rather than a single connection) might not be detected.

  Note, though, that when looking at aggregated information and reports, these limitations are of less significance, due to averaging and aggregation of large number of calls.

Resolution Limitation on Quota Breach Detection

- Cisco number: 10470

  The SCA BB application performs per-session enforcement on fixed time intervals. This means that quota breach detection and the corresponding policy enforcement take place with this predefined accuracy (default is 30 seconds).

  Workaround: This is the normal system behavior, described for clarification. When defining quota breach rules, expect up to 30 seconds (or the configured duration set in the ongoing-policy-check option) during which a subscriber may exceed quota before enforcement is performed.

Reporting Volume of Bundled Flows on Multiple Links

- Cisco Number: 13647

  Certain types of network sessions are composed of several network connections, or flows. SIP and FTP, for example, use one network flow for control, and additional flows for data. When working with the SCE2000 platform in multiple link topologies, it is possible that flows of the same session can be carried on separate links. For example, a SIP control flow may be carried on Link 1, while the data flows may use Link 2.

  In this case, the volume of the session's flows reported in Link Usage RDRs is reported on the link of the first flow. This can potentially lead to inaccurate global volume and bandwidth reports per link in the Reporter, though the total volume and bandwidth reports will remain accurate.

BW Reports May Contain Spikes after DoS Attacks

- Cisco number: 10822

  When the SCE detects a DoS attack, the bandwidth reports might show a “spike” in the Generic TCP traffic (that is, a significant increase in traffic) at the time when the attack subsided.

  Workaround: When reviewing the reports, be aware of this phenomenon.

Application Management, Configuration and User Interface

New Protocols Not Assigned Automatically to Services in Old PQB Files

- Cisco Number n/a

  When upgrading old PQB files, Skinny, MGCP, Yahoo Messenger and DingoTel 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: To fix this, manually assign the above protocols and the new ones to a service using the SCA BB Console.

Format of Subscriber State in Release 2.5 Incompatible with 2.1

- Cisco Number n/a

  The SM stores a state for each subscriber in its subscriber database. The SM sends this state to the SCE platform when the subscriber logs in. The subscriber state is an object that has different formats in versions 2.1 and 2.5. Therefore, during an upgrade from 2.1 to 2.5, when the SM sends the subscriber state in 2.1 format to a 2.5 SCE platform, it results in multiple errors in the SM and SCE logs.

  Workaround: The solution is to clear all the subscriber states from the subscriber database on the SM as part of the upgrade process. This procedure is described in the SM User Guide. To do this, the ‘p3subsdb’ SM CLU is used as follows:

  ```
  P3subsdb –clear-all-state
  ```

Dropped Packets/Bytes Counters Unavailable in SCA BB MIB

- Cisco Number: n/a

  The SNMP interface of the SCE shows the MIB, which provides access to application counters. In previous SCA BB releases, this included counters of dropped packets and dropped bytes per service, in link and package scopes. These counters are no longer available in this release.

  Workaround: None

Export/Import Packages to CSV Files Unavailable in SCA BB Console

- Cisco Number: n/a

  The SCA BB Console no longer supports importing and exporting of packages to CSV files (Importing and exporting lists, protocols and services is still supported.). Due to the complex structure of SCA BB Packages in this release (Rule hierarchy, BW Controllers, Quota Buckets, etc.), a CSV table cannot be used. A replacement is planned for future releases, where importing and exporting of packages to XML files will be supported.

  Workaround: None

Subscriber Notification on DoS Attacks Removed on PQI Installation

- Cisco number: 11773

  PQI installation of a new SCA BB revision removes the settings of Subscriber Notification on Network Attack.

  Workaround: When possible, perform a PQI upgrade instead of a PQI installation. Verify Subscriber Notification settings after performing a PQI upgrade or install.

Transactions Not Properly Mapped for Generic TCP/UDP

- Cisco number: 8391

  Transactions will not be mapped properly if the service is defined by the Generic TCP/UDP protocol and IP address list, if a more specific service exists, as defined by a Port-based protocol with the initiating side and the same IP address list.

  The following scenario is an example of when the transactions may not be mapped properly:

  Service Configuration contains these 3 services:

  - "Subscriber-Initiated Local Gaming" - Subscriber-initiated transactions using a port-based protocol to a "local servers" IP address list.
  - "Both-Ways Local Generic TCP" - Generic TCP transactions to/from the same "local servers" IP address list.
  - "Generic TCP" default service.

    Network-initiated transactions that should have been classified as "Both-Ways Local Generic TCP" (2) will be classified as "Generic TCP" (3).

Editing Service Transaction Mapping Can Clear List Selection

- Cisco number: 10609

  When editing a Service's transaction mapping in the SCA BB Console, selecting a protocol clears the lists selection. The usual order of configuration is to select the protocol, then to select an initiating side and finally selecting lists. If the order is not followed and a protocol is selected after the lists, the lists are cleared.

  Workaround: When changing the protocol of a transaction mapping with lists, re-configure the lists after the protocol change.

Persistent Storage of Service Configuration Might Fail

- Cisco number: 10609

  In rare circumstances, the persistent storage of Service Configuration on the SCE Platform fails, though the new configuration is applied. This means that after SCE reboots, the configuration is reset to its previous state. When this happens, the SCA BB Console displays an error message in its message pane, prompting the user to apply the configuration again.

  Workaround: Re-apply the service configuration if you receive the following error message:

  ```
  ERROR: Persistent storage of the Service Configuration on the SCE has failed
  ```

Connecting the SM GUI to the SM Requires an FTP Server on the SM

- Cisco number: n/a

  In order to connect to the SM, the SM GUI requires that the FTP server on the SM machine be enabled on port 21. The connection password is that of the pcube account.

Microsoft Excel May Invalidate Format of SCA BB CSV File

- Cisco number: 10658

  SCA BB CSV files are composed of rows of comma-separated values. When the values in the end of a row are empty, they are denoted with consecutive commas. Excel removes these consecutive commas at the end of a CSV row. This makes the file's format invalid and its content cannot be imported back to SCA BB.

  Workaround: Add the missing commas a text editor before importing.

API Issues

Unneeded Connections Should Be Closed

- Cisco number: 10580

  When using the SCA BB API, it is important to properly close SCE connections that are no longer needed and minimize number of concurrently open connections.

  SCA BB API can be used to automate Service Configuration tasks, such as opening a connection to an SCE platform and applying a Service Configuration files. As each connection consumes resources on the SCE device, it is necessary to properly close any connection opened during the process. Additionally, whenever possible try to reuse a single connection instead of opening multiple ones

  Workaround: When programming with SCA BB API, refrain from creating multiple simultaneous connections to the same SCE. Try to reuse an existing connection. Make sure to properly close the connection by calling the logout method.

Installation

RPC Server Error

- Cisco number: 10637

  When launching the SCA BB clients' setup on a Windows PC, the following error message may appear: `The InstallShield Engine (iKernel.exe) could not launch - The RPC server is unavailable`.

  Workaround: In Windows, select **Start** > **Run** and type **`net start rpcss`** in the 'Open' box, and then click **OK**. Test to see if this resolves the issue. If the issue still occurs, restart your PC and launch the setup again.

Data-Collection and Reporting

Data-Collection Software: Warning Message in Output of ./dbperiodic.py --load

- Cisco number: 9959

  The following warning massage might appear when running the script **`./dbperiodic.py --load`**:

  ```
  warning - could not read existing crontab. proceeding anyway...
  ```

  Workaround: Ignore the message.

DC/Reporter Does Not Enforce Maximum Number of Open Connections

- Cisco number: 10791

  The Reporter does not enforce the maximum number of active connections (that is, open report windows) the user can create. Therefore, on rare occasions, when opening many concurrent reports in the Reporter, if the number of possible connections is almost reached, if the DC DB adapter happens to be restarting at this time, it may get connection refusals from the DB because there are not enough available connections.

  Workaround: If there is an indication in the DC log about failures to connect to the database, and you have a Reporter open with many active windows, close the reporter and restart the DC. (Note that if the *sudo* package is installed on the DC, the DB Adapter will do this automatically by restarting the database).

US English locale must be used

- Cisco number: n/a

For correct SCA BB and Sybase operation, English locale must be used.

Workaround: Set the locale.

To set the locale:

Step 1. Add to the */etc/TIMEZONE* configuration file, the line: **LANG=en_US**.

You must reboot in order for the changes in the file to take effect.

Step 2. Install this locale in Solaris.

To verify if it is installed check if the following directory exists*: /usr/lib/locale/en_US*. If it does not, install the locale from the Solaris CD's

Posix format for time zone not recommended

- Cisco number: n/a

  Setting the OS time zone as an offset from GMT in POSIX format is not recommended and may lead to problems in future versions.

  Workaround: It is best to set the time zone in the */etc/TIMEZONE* configuration file by (supported) country name, for example: **TZ=Japan**

  You can verify that the country name is supported as a time zone setting by checking that it is listed in the directory */usr/share/lib/zoneinfo*.

  In case GMT offset must be used, use the "zoneinfo" format by prepending an '*:Etc/'* *prefix*, for example: **TZ=:Etc/GMT+5**

Reporter Tool

Saved Report Templates May Be Unusable After Policy Change

- Cisco number: 10735

  Generating a report from a saved query after applying a new policy to the SCE with new services, could fail with a database error.

  Workaround: Modify the saved queries to ensure that the service names used are those currently available.

Duplicate Names in Top Service Ports Report

- Cisco Number: n/a

  While generating the “Top Service Ports” report, only the port-number and the default associated protocol displays in the chart-view. This causes port numbers used by multiple protocols (such as port 80 used for HTTP and KazaA) to show the same legend in the chart (80(http) in this case).

  Workaround: Switch from chart view to table view so that the service name can be seen in addition to the name associated with the port.

Tables Always Print on the Default Printer

- Cisco number: 5049

  Tables always print on the default printer.

  Workaround: Change the printer settings.

  To change the settings:

Step 1. From the Taskbar, select Start>Settings>Control Panel>Printers.

The list of printer icons is displayed.

Step 2. From the list of printer icons, right click the one you wish to print the table to.

Step 3. From the popup menu, select **Set as Default Printer.**

The Help Button in the "Reports Wizard" does not Function

- Cisco number: 5282

  The Report Creation Wizard contains a Help button. Pressing this button does not open a help window.

  Workaround: There are no known workarounds.

The Find Function in the Reporter Table View is not Functional

- Cisco number: 8111

  The documented “Find” operation on a table view does not work.

  Workaround: There are no known workarounds.

Opening the Reporter without Templates Provides no Indication

- Cisco number: 9092

  While the Reporter runs without the templates installed, the only indication of the situation is the appearance of the Report generation wizard with an empty templates box.

  Workaround: Ensure that you properly install the SCA BB templates after installing the reporter.

  To verify that the templates are installed:

Step 1. From the Taskbar, select **Start>Settings>Control Panel>Add/Remove Programs**.

Step 2. Search for **Cisco SCAS Reporter Templates**

A "Reporter DB Error" may Pop Up, when refreshing a Report Window

- Cisco number: 8015

  In extremely rare circumstances, refreshing a report window causes an error message to pop up.

  Workaround: Close the wizard and then re-open it.

Printing a Preview of a Table (not a Chart) Causes the Table to Disappear from the Report

- Cisco number: 8106

  Creating a preview of a table from a chosen report, and then minimizing the print preview, causes the table to disappear from the report window it was created in.

Step 1. Maximize the **Preview** window or reactivate print preview.

Step 2. Click the **Close** button.

The preview window closes and the table reappears.

A Report Cannot Close while it is Produced

- Cisco number: 8128

  While the reporter queries the database in order to create the requested report, the report window cannot close; thus the creation of the report cannot be interrupted.

  Workaround: In case you must interrupt the query, close the Reporter application using the windows Task Manager, and then restart it.

Clicking the Report Button while a Query is Running may Abort the Query

- Cisco number: 8131

  In extremely rare circumstances, when you simultaneously, generate a report, and click the Report button to generate another report, an error pops up and the first report is not displayed.

  Workaround: There are no known workarounds.

Table Values in the Reporter Cannot be Copied to the Clipboard

- Cisco number: 3116

  While viewing a report in a table format, you cannot copy the table content to the clipboard.

  Workaround: Perform the following steps:

Step 1. Export the contents of the table to a file.

Step 2. Open the file in a text editor or a spreadsheet application.

Step 3. Copy the content to the clipboard.

To copy the contents of one cell, select **CTRL**+**Insert.**

The Reporter Displays the Word "Engage" Occasionally in the SCE IP Line

- Cisco number: 10137

  In rare circumstances, when starting the Reporter, the SCE IP dialog box displays the word “Engage”.

  Workaround: Prior to login ensure that the SCE IP box contains an actual list of IP’s. Click the ‘**…**’ button to view the list..

Single Quotes Cannot be Used in Arbitrary Strings in the Reporter

- Cisco number: 10287

  The Reporter cannot use a single quote in queries involving arbitrary strings (for example, subscriber names). If such a string is used, an SQL error occurs.

  Workaround: Do not use single quote characters in subscriber names, package names, etc.

Empty choices fields when trying to create new report after first reporter installation

- Cisco number: 14192

  At rare circumstances, when starting the reporter at the first time after installation and trying to generate new report some of the report choices fields are empty, for example the choice field called "traffic direction" appear with no selection options.

  Workaround: Reopen the reporter.

Documentation Errors

Empty Info String in Blocking RDRs on SMTP / POP3 / NNTP

- Cisco Number10515, 10516, 10517

  The info string for SMTP, NNTP & POP3 is incorrectly documented to contain value in the layer-7 fields for the BLOCKING_RDR. This is not the case and the fields are reported empty (because blocking occurs prior to the information being sent).

  It is important to note that transaction RDRs, on which many reports are based, convey the corresponding info strings correctly.

Limitations on List Items and Protocol Ports in Service Configuration

- Cisco Number: n/a

  The documentation does not accurately define the list items maximum size:

  - Max number of list items: 10,000 items.
  - Max number of protocol ports: 5000 ports.

  The system will display an error if the service configuration exceeds the limits.

Incorrect Licensing Documentation

- Cisco Number: n/a

  The SCA BB User Manual incorrectly documents a license for “capacity-control” and one for “tiered-control”. This is incorrect, and only the “tiered-control” license exists.

Obtaining Technical Assistance

Cisco provides *Cisco.com* as a starting point for all technical assistance. Customers and partners can obtain documentation., troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://tools.cisco.com/RPF/register/register.do

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.